IDT Series

Law and Web 2.0

Proceedings of the First Workshop on Law and Web 2.0

Organized by:
IDT – Institute of Law and Technology (UAB)

In cooperation with DerechoTICs

Antoni Roig (Ed.)
Cristina García. Conference Support – IDT

Barcelona, Spain
September 18, 2009

IDT Series

Series Editors:

Pompeu Casanovas
Núria Casellas
Pablo Noriega
Marta Poblet
Antoni Roig
Joan-Josep Vallbé

Volume 3

Law and Web 2.0
Proceedings of the First Workshop on Law and Web 2.0.

Volume Editors: Antoni Roig (Ed.)
Linguistic revision: Sílvia Gabarró López, Elisenda Casañas Adam
IDT Administration: Cristina García Gálvez

Acknowledgements: TSI-020501-2008-131; TSI-020100-2008-134; CSO-2008-05536-SOCI; CEN2008-1018; AGAUR-SGR-2009

ISSN: 2013-5017
Legal Deposit: B-37745-2009

Editors' addresses:

Institute of Law and Technology
School of Law
Universitat Autònoma de Barcelona
08193 Bellaterra, Spain
marta.poblet@uab.cat

Derecho TICs
Universitat de Valencia
Edificio departamental central
Despacho 1 E 02
Avda. de los Naranjos s/n
46071 Valencia
cotino@uv.es

© 2009 The authors
© 2009 The volume editors
© 2009 UAB Institute of Law and Technology

Publisher:

Huygens Editorial
La Costa 44-46, át.1ª
08023 Barcelona. Spain.
www.huygens.es

Foreword: A Fruitful Cooperation

It is a pleasure to introduce the results of the Workshop on Law and Web 2.0, organized and conducted by Professor Antoni Roig.

It is usually stated that the term *Web 2.0* emerged from a 2004 brainstorming session among officials of O'Reilly Media, Inc. and MediaLive International.[1] Actually it was used a bit earlier as a label or a way of speaking.[2] It is currently referred as "the social web", the opening of the web to people participation. Flickr, YouTube, Wikipedia, Facebook… are well known and universally praised examples of it.

However, even a celebrated technological advance such this one is not free from side effects. Sensitive data, privacy, safety and the possibility of misconducts on the Web seems to be the issues at stake.

The Workshop held on September 18th at the UAB addresses these fundamental issues in a new way. It seems to me that the fruitful cooperation between IDT researchers and DerechoTics members fostered by professor Roig has a worthwhile feature: instead of focusing on regulation alone, or on the legal aspects of privacy, Dr. Roig opens up the field to the straight entrenchment of law and technology.

Therefore, the reader will find out in the following pages useful information on technical protocols, computational problems, and upcoming software. This is an added value to the legal knowledge and ethical issues addressed in the next three sections on privacy, free speech and ISP accountability.

Thanks to all the participants for their good work and well oriented efforts.

Pompeu Casanovas
Director of the UAB Institute of Law and Technology

1. D.E. Harmon, "The 'New' Web: Getting a Grip on the Slippery Concept of Web 2.0", *Lawyer's PC*, vol. 23, n. 1, 2006, pp. 1-5.
2. *Cfr*. E. Knorr, 2004 – *The Year of Web Services, IT magazine CIO*, December 2003, p. 90, at http://books.google.com/books?id=1QwAAAAAMBAJ&printsec=frontcover&source=gbssummary_r&cad=0_0#PPA90,M1 (accessed 12 May 2009).

Contents

Section 1 – Privacy and web 2.0

Privacy and Social Network Applications 1
Antoni Roig (IDT-UAB)

Applications to Improve Privacy on Online Social Networks. 17
Víctor Rodríguez, Anna Carreras, Eva Rodríguez and Jaime Delgado (DMAG-UPC)

Privacy Features of Authentication Systems 35
J. Herranz (UPC), J. Iñigo and H. Pujol (Safelayer)

Section 2 – Free Speech and web 2.0

Dissemination of information under neutrality principle in Spain 47
Carles Alonso (UB-Catalan Agency of Certification)

Privacy and free speech in social networks. 63
Luis Fernando Rodríguez García (UNED)

Section 3 – ISP Accountability and web 2.0

The problem of liability for illegal content in the web 2.0 and some proposals . 73
Lorenzo Cotino Hueso (UV-DerechoTICs)

Service Providers Accountability 85
Sergi Torralba, Albert Meroño, Antoni Roig (IDT-UAB)

Section One
Privacy and Web 2.0

Privacy and Social Network Applications[1]

Antoni Roig

Researcher of the IDT (Law and Technology Institute)
of the Autonomous University of Barcelona

Abstract. Privacy technological threatens are no limited to data protection. Social Network Applications (SNA) and ubiquitous computing or Ambient Intelligence face other privacy risks. The business model of SNA and the improvement of data mining allow social computation. SNA regulation should favor privacy-by-design and Privacy Enhancing Technologies (PET). Default friendly-privacy policies should also be adopted. The data portability of the applications shifts SNA into a new field of ubiquitous computing. Therefore, the solutions of the Ambient Intelligence shoud be also analysed in the context of SNA.

Keywords: Social Network Applications, Privacy, Privacy Enhancing Technologies, Privacy-by-Design, Ubiquitous Computing, Ambient Intelligence.

1. Major Privacy Concerns

1.1. Control

Personally Identifiable Information (PII) is willingly provided by users of Social Networks Applications (SNA). So one of the major privacy concerns is the lack of self-control over these data. In fact, the business model of the SNA consists of exploiting the value of users' PII. A recent study gives us a more precise idea of the amount of PII introduced in the SNA (Fogel, Nehmad, 2009). More than three-quarter of students have created a social networking profile in Facebook, and about one-half in MySpace. The average years for the profile displayed was 1.9 years. With regard to a daily visit to one's profile, the average was 2.4 times. Other profiles were viewed on average 4 times. Concerning daily hours spent viewing profiles, the average was 1 h. The average number of "friends" on profiles was 239. Almost three-quarter allowed anyone to view their profile without restricting views to those specifically accepted. Almost 10% included their phone number and home address on their profile.

1. This study is within the frame of the funded research project "Freedom of speech In the Context Of Web 2.0 and Social Networks: Redefinition, Guarantees and Limits", Cotino as main researcher. Ministry of Science and Innovation (DER2009-14519-C05-01).e

The "News feed" and "Beacon" features in Facebook are interesting examples of control concerns. Facebook released the News Feed feature on September 5, 2006. The feature culls new PII that users post on their personal profile pages and delivers it to the website's initial page (Hoadley, C. M. *et al.*, 2009): for instance, "Alice's status changed from 'single' to 'in a relashionship'." Facebook indicated that it would make new information easier than ever to find. In response to the widespread concerns, Facebook immediately took down the News Feed applications and worked nonstop for two days on providing a wider variety of privacy preferences. Then Facebook re-released the News Feed applications with new privacy control features. On September 8, 2006, Facebook's CEO, Mr. Zuckerberg, apologized for this privacy outcry and said: "this was a big mistake on our part, and I'm sorry for it. . . But apologizing isn't enough. I wanted to make sure we did something about it, and quickly. So we have been coding nonstop for two days to get you better privacy controls."

With News Feed, no new information was revealed; users could only see changes of their friends' pages. So, why were users so uncomfortable with it? A plausible explanation is that the new interface offered lesser levels of perceived control over PII (Xu, H., 2009). One possible conclusion is that privacy concerns can be lessened by offering more control functions: first of all, control of PII disclosure; but also control access to disclosed information. With News Feed, obtaining information about other users was easier, which leads to a lower perception of control.

1.2. Transparency

Online privacy policies are difficult to understand. Most privacy policies require an ability to decode legalistic, confusing, or jargon-laden phrases. Privacy researchers and industry groups have thus devised several standardized privacy policy formats to help people compare policies (McDonald, A.M. *et al.*, 2009).

Another helpful tool that shows what a user is sharing with whom is Facebook's profile preview tool[2]. Go to *Settings' Privacy Settings,* then *Profile,* and type a friend's name in the box on the top. You will see your profile as that friend would view it, and then you can adjust your privacy settings accordingly (Larkin, 2009).

1.3. Unauthorized use

Facebook states that it will do everything possible to protect the information posted on the site but "cannot and do not guarantee that User Content you post on the Site will not be viewed by unauthorized persons" (Facebook, 2009). Indeed, we will see later that other users or even non-users can accede and use PII most of the time from SNA users.

2. Other interesting tools for Facebook users at Nick O'Neill's "10 Privacy Settings Every Facebook User Should Know", www.allfacebook.com/2009/02/facebookprivacy.

2. Legal Framework

2.1. Data protection regulation

Data protection regulations are considered by some authors as a reference basis for the development of methodologies tailored to design privacy-aware systems (Guarda, Zannone, 2009). The first step is to summarize the privacy principles:

(1) Fair and Lawful Processing: the collection and processing of personal data shall neither unreasonably intrude upon the data subjects' privacy nor unreasonably interfere with their autonomy and integrity, and shall be compliant with the overall legal framework.
(2) Consent: personal data shall be collected and processed only if the data subject has given his explicit consent to their processing.
(3) Purpose Specification: personal data shall be collected for specified, lawful and legitimate purposes and shall not be processed in any way incompatible with the purposes for which data have been collected.
(4) Minimality: the collection and processing of personal data shall be limited to the minimum necessary for achieving the specific purpose. This includes that personal data shall be retained only for the time necessary to achieve the specific purpose.
(5) Minimal Disclosure: the disclosure of personal data to third parties shall be restricted and only occur upon certain conditions.
(6) Information Quality: personal data shall be accurate, relevant, and complete with respect to the purposes for which they are collected and processed.
(7) Data Subject Control: the data subject shall be able to check and influence the processing of his personal data.
(8) Sensitivity: the processing of personal data, data which are particularly sensitive for the data subject, shall be subject to more stringent protection measures than other personal data.
(9) Information Security: personal data shall be processed guaranteeing a level of security appropriate to the risks presented by the processing and the nature of the data (Guarda, Zannone, 2009).

2.2. Recommendations

Up to now, one report of 2008 is perhaps the most relevant legal framework on WBSN and privacy ("Rome Memorandum"). One key legal preliminary consideration is that there are only very few rules governing the publication of personal data at the initiative of private individuals. This is due to the fact that it had not been a major issue in the real world, and it has been only rel-

evant on the Internet with WBSN. Another sociological key element is that a new generation of "digital natives" has appeared, and they seem more comfortable with publishing (sometimes intimate) details of their lives on the Internet. The Rome Memorandum recommendations to regulators are:

- Introduce the option of a right to pseudonymous use.
- Ensure that service providers are honest and clear about what information is required for the basic service. Specific problems exist with consent of minors.
- Obligation to data breach notification for social network services.
- Possibly attributing more responsibility to WBSN providers for personal data content on WBSN.
- Improve integration of privacy issues and tools into the educational system.

Another interesting document is the European Network and Information Security Agency Position Paper 1. Some of the recommendations are:

- WBSN should, where possible, use contextual information to educate people in 'real-time'.
- Awareness-raising campaigns should also be directed at software developers to encourage security conscious development practices and corporate policy.
- The regulatory framework governing WBSN should be reviewed and, where necessary, revised:
  - What is the legal position on deletion of user generated content by service providers if it is classed as WBSN spam?
  - What is the legal position on image-tagging by third parties?
  - Who is responsible for security flaws resulting from user-generated markup or scripting?
  - How should privacy policies of embedded third party widgets be communicated to users?
  - What exactly constitutes personal data in a WBSN environment?
  - What is the legal position on profile-squatting?
  - Should the posting of certain classes of data by minors (location data) be made illegal?
- Users should be given accurate information on what is done with their data before and after account closure. WBSN should be used in a controlled and open way (i.e. not banned or discouraged) with co-ordinated campaigns to educate students, teachers and parents.

Recently, we can mention the Working Paper n°163 of the article 29 Group dealing with online social communities, June 12, 2009[3]. This study considers that the European Directive of data protection covers also the SNA scenario:

"The new aspects of this recommendation are perhaps the reference to security tools and "privacy-friendly" default settings. For the first time, a recommendation mentions Privacy Enhancing Technologies as a solution, even if limited to the problem of the privacy of young users."

2.3. Beyond data protection

But privacy cannot be limited to the data protection regulation. The German Constitutional Court published a decision in February 2008. This decision constitutes a new "basic right to the confidentiality and integrity of information-technological systems" as part of the general personality and privacy rights in the German constitution[4]. The ruling explains the relevance of using information-technological systems for the expression of personality. These systems are defined as technological tools that "alone or in their technical interconnectedness can contain PII of the affected person in a scope and multiplicity such that access to the system makes it possible to get insight into relevant parts of the conduct of life of a person or even gather a meaningful picture of the personality". Weiss considers that this description could be easily applied to social network profile data (Weiss, 2009).

3. Privacy Preserving Tools and Procedures

3.1. SNA need new PETs

At least, the ISO has achieved consensus on four components of privacy as follows (Wright *et al.*, 2009):

- Anonymity ensures that a subject may use a resource or service without disclosing user identity.
- Pseudonymity ensures that a user may use a resource or service without disclosing identity, but can still be accountable for that use.
- Unlinkability ensures that a user may make multiple uses of resources or services without others being able to link these uses together.

3. Opinion 5/2009, on online social networking, available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm

4. BVerfG, 1 BvR 370/07 from 2008-02-27, paragraph (1–333), http://www.bverfg.de/entscheidungen/rs20080227 1bvr037007.html.

– Unobservability ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used[5].

General Privacy Enhancing technologies, like anonymity, pseudonymity, and access management are useful for surfing the Internet. Nevertheless, SNA do not seem a priority because the increasing of the PII is at the core of business model. This a major problem for PeerSoN, a decentralised SNA based on Peer-to-Peer (Buchegger *et al.*). More, privacy in SNA can not be considered as data protection, and thus be limited to access control and processing of data. Anonymity is not completely abandoned (Kacimi *et al.*, 2009) and access control can be managed with semantic web framework (Carminati *et al.*, 2009). We can also adapt interesting cryptographic solutions to Facebook (Lucas, Borisov, 2008). The main aim of cryptographic solutions is to what extent a user can ensure his privacy while benefiting from existing online services. NOYB is a novel approach that provides privacy while preserving some of the functionality provided by online services (Guha *et al.*, 2008). The identity management can also be improved by reputation systems adapted to SNA, which are platforms of several online communities linked such as Facebook (Pingel and Steinbrecher, 2008).

However, SNA need new PETs focused on transparency, automatic compliance assurance functions and proactive communications techniques on risks (Weiss, S., 2009).

3.2. Transparency

The complete transparency and control of the usage of the user's PII is only possible with privacy-by-design practices for designers and developers. PETs cannot be simply an added tool, but have to be incorporated at the first stages of the design or the application development. For instance, *PriS* is an engineering method which incorporates privacy requirements early in the system development process (Kalloniatis et al., 2008). Privacy requirements are considered as organisational goals that need to be satisfied. *PriS* provides a description of the effect of privacy requirements on business processes, and it allows the identification of the best privacy-preserving system architecture.

3.3. Default privacy settings

A recent study shows that while there is some use of privacy settings by SNA users now, there is still a significant portion of SNA users who have not

5. ISO/IEC 15408, Information technology – Security techniques –Evaluation criteria for IT security, First edition, International Organization for Standardization, Geneva, 1999. The standard is also known as the Common Criteria.

changed their permissive settings and allow unknown users to view private bits of information. SNA must clearly indicate the bare minimum of private information needed for a particular set of interactions (Krishnamurthy *et al.*, 2008). The default privacy settings should be the bare minimum. Furthermore, a privacy tool to identify the metrics bare minimum would be useful. It would also allow users to compare various SNA with a clear comparative element of analyses (Krishnamurthy *et al.*, 2008).

Another aspect of the problem is helping a new user to identify suitable default privacy settings. An interesting tool allows a choice of default privacy settings that have been learnt from a set of users' privacy settings. This solution has the advantage that users can easily understand and modify these settings to specify their desired initial policy (Ravichandran *et al.*, 2008).

The adoption of a sort of proactive communication would be also useful. Indeed, there should be options for the user to easily report privacy invasions.

4. New challenges: Data Portability

Data mining and screen scrapping applications automatically infer real-word connections, and discover communities and individuals. Indeed, identifying consumer preferences is a key challenge in customizing electronic commerce sites to individual users. People linked in SNA often share preferences, allowing inference of interest in products based on knowledge of a consumer's network friends and their interests (Hogg, T., 2009). SNA operators should also be aware of the importance of not only protecting user profile data, but the structure of the social graph. In September 2007, Facebook started making public search listings available to those not logged in to the site to encourage visitors to join the SNA. A recent study concludes that they should not assist data aggregators by giving away public listings because it allows data retrieval. (Bonneau *et al.*, 2009). Another way of getting PII, particularly link privacy attack, uses the lookahead tool that indicates the friends known by a user. A recent study suggests SNA not to limit the lookahead to 1 or 2, whenever possible (Korolova *et al.*, 2009). An extreme use of SNA, the so-called *Antisocial Networks*, are distributed systems based on social networking Websites that can be exploited by attackers and aimed at carrying out network attacks (Athanasopoulos, 2008). These examples are external discovery or disuse of PII.

The problem comes also from the inside. PII data from SNA have more and more applications to run with or "mash up" applications. In fact, a recent study found that about 90% of the top 150 Facebook applications get access to PII which should not be allowed to manage (Felt, Evans, 2007). Some possible privacy improvements in Facebook: one Facebook user can see the applications he has currently authorized going to *Settings-Application Settings* (Larkin, 2009). If a friend installs an application, the program will be able by default to see anything a user has shared with that friend. To restrict the data available, a user can go to *Settings-Privacy Settings* and click the *Applications* link. Then,

he can click the *Settings* tab on the top, and deselect any checked boxes on that page for info he doesn't want to be shared. These settings only affect the applications his friends have installed. Afterwards he has to choose *Authorized* from the 'Show' drop-down menu (Larkin, 2009).

Google announced the adoption of standards such as Friend-Of-A-Friend (FOAF) and XHTML Friends Network (XFN) in their OpenSocial application to give access to the developers to the network graph, i.e. the map of connections between friends. This is data portability based on known standards, but in many cases there is no standard guidelines in the process.

That is the reason why Weiss proposes a privacy threat model for SNA portability (Weiss, 2009):

- Information privacy needs to be controlled on the data (PII) level.
- The user needs to be able to determine the sensitivity and context of the PII provided.

This seems a major challenge when we read about impressive tools such as CenceMe. CenceMe injects sensing presence into popular social networking applications such as Facebook, MySpace, and IM (Skype, Pidgin) allowing new levels of "connection" and implicit communication (albeit non-verbal) between friends in social networks. Sensing presence captures a user's status in terms of his activity (e.g., sitting, walking, meeting friends), disposition (e.g., happy, sad, doing OK), habits (e.g., at the gym, coffee shop today, at work) and surroundings (e.g., noisy, hot, bright, high ozone) (Miluzzo *et al.*, 2009). An interesting solution for the context problem is DroPicks (Hosio *et al.*, 2007). The context is defined by the fact that many everyday artefacts are immobile, which implicitly restricts contents stored in a location. Such indirect, contextual sharing has advantages over direct communication mechanisms (E-mail, SMS, IM...).

• Privacy-preserving data portability can only work if the user can earmark the PII provided with individual privacy preferences.

In order to respect individual privacy preferences, the user self-control and the ease of public accessibility, further research is announced on semantic technologies for tagging data for context and purpose, transparency-enhancing technologies and Digital Rights Management (Weiss, 2009).

5. Future Trends: Privacy and Ubiquitous Computing

The deployment of ubiquitous computing casts doubt on the extent to which privacy is legally protected in public spaces (De Hert *et al.*, 2009). In case law, the European Court of Human Rights has introduced the notion of "reasonable expectation of privacy". But ubiquitous computing is turning the reasonable expectation of privacy into an expectation of being monitored. Furthermore,

pervasive computing needs as many data as possible which clearly clashes with some of the main principles of data protection law. For instance, the data minimisation principle, collecting as little data as necessary, and the purpose specification principle only use the collected information for the purpose defined at the moment of data collection (De Hert *et al.*, 2009).

With the emergence of Ambient Intelligence or pervasive computing, the definition of personal data needs to be reconsidered (Wright *et al.*, 2009). Moreover, the distinction between personal and other data in a ubiquitous computing world is difficult to maintain. Perhaps it is time to data protection *tout court*. Indeed, the definition of personal data more and more implies the necessity of a case-by-case assessment, an approach upheld in a recent opinion from the Article 29 Data Protection Working Party on the definition of personal data[6]. With ubiquitous computing, a new net, the Internet of things, will link many "anonymous" data to persons. Therefore, a lot of data mining and analyses will follow. As a result, all data will be personal data (Wright *et al.*, 2009). In fact, in many cases it would not be even necessary to identify an individual in order to conduct commercially profitable operations. The unique identifier will be enough for intrusive marketing, for instance. So instead of identifiability as a criterion, privacy relevant data should rather be all those that can be used to affect our behaviour and decisions (Wright *et al.*).

Another important issue is the transparency of the processing. According to data protection regulation, data collectors and data processors should indicate the user which data are collected and give him or her basic information about the data processing. Nowadays, the user has not a comprehensive view of the data processing and its implications. In any event, such an information requirement might be unworkable with the generalization of the ubiquitous computing (Wright *et al.*, 2009). What will become important in the context of SNA is the profiling knowledge, that is to say the access to the profile. This information could make comprehensible why the environment takes some actions, and could even help to prove liability in case of damage (Wright *et al.*, 2009). On the other hand, anonymity can also be a useful tool with mobile community services (Demestichas, K. *et al.*, 2009). PETs could provide important factual means of transparency. Transparency-enhancing technologies (TETs) could contribute to information exchange and management. An example of a TET is the so-called "sticky policies", which stick to or follow data as they are disseminated[7]. Sticky policies would provide clear information and indicate to data processors and controllers which privacy policy applies to the data concerned (De Hert *et al.*, 2009).

6. Article 29 Data Protection Working Party, Working document on data protection issues related to RFID technology, 10107/05/EN, WP 105, 2005. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf.

7. Hildebrandt M, Meints M (eds) (2006) RFID, profiling, and AmI, FIDIS (Future of Identity in the Information Society) Deliverable D7.7. http://www.fidis.net

The privacy concern about cloud computing can be a good analogy. As cloud services process users' data on machines that the users do not own or operate, recommended privacy practices for developers are welcome (Pearson, 2009):

1. Minimise personal information sent to and stored in the cloud
2. Protect personal information in the cloud
3. Maximise user control
4. Allow user choice
5. Specify and limit the purpose of data usage
6. Provide feedback

Particularly, for mobile, ubiquitous social awareness applications, other complementary principles are (Raento, Oulasvirta, 2008):

1. Support lightweight permissions
2. Assume reciprocity
3. Make it possible to appear differently to different people
4. Allow for commenting, modifying and framing automatic disclosure
5. Provide for feedback
6. Allow the user to lie
7. Do not take control away from the user
8. Allow opportunistic use
9. Do not try to do everything within the system

In any case, Ambient Intelligence, or ubiquitous computing, requires a shift to privacy-by-design and PETs (Wright *et al*., 2009). Regulatory authorities and/or industry leaders could usefully encourage or formalise this option. Some research consortia, under the European Commission 6th Framework Programme, are good examples[8].

6. Conclusion

No single measure will adequately respond to the challenges to privacy posed by SNA and the ubiquitous Information Society. In fact, some combination of measures will be needed (Wright *et al*., 2009). Privacy principles, like Fair Information Principles (FIPs) or data protection principles are not enough. Perhaps, we are witnessing the very first stages of an important shift: the proportionality and transparency can wide the traditional data protection

8. Some deliverables are DISCREET Deliverable 2402, March 2008, http://www.ist-discreet.org/ and SPICE Deliverable 1.8, May 2008. http:// www.ist-spice.org/nav/deliverables.htm.

principles. But, if we want to face to new possibilities of data portability or ubiquitous computing, we have also to encourage the adoption of PETs and TETs. Furthermore, this has to be done with privacy-by-design practices and not in a second moment of the implementation. We can go on indicating how these changes are transforming the privacy right, but perhaps it is time now to analyse and offer concrete solutions to concrete SNA. This should require a deep study of the privacy policies of a concrete SNA, and work together in the design of future applications, adopted with privacy-by-design practices.

References

1. Athanasopoulos, E., Makridakis, A., Antonatos, S., Antoniades, D., Ioannidis, S., Anagnostakis, K.G. and Markatos, E.P. (2008), Antisocial Networks: Turning a Social Network into a Botnet, in T.-C. Wu et al. (Eds.): ISC 2008, LNCS 5222, pp. 146–160, 2008.
2. Bonneau, J., Anderson, J., Anderson, R. and Stajano, F. (2009), Eight Friends Are Enough: Social Graph Approximation via Public Listings, SNS '09 Nuremberg, Germany.
3. Buchegger, S., Schiöberg, D., Vu, L.-H and Datta, A. (2009), PeerSoN: P2P Social Networking. Early Experiences and Insights, SNS'09, March 31, 2009, Nuremberg, Germany.
4. Carminati, B., Ferrari, E., Heatherly, R., Kantarcioglu, M. and Thuraisingham, B. (2009), A Semantic Web Based Framework for Social Network Access Control, *SACMAT'09,* June 3–5, 2009, Stresa, Italy.
5. Demestichas, K.P., Adamopoulou, E. A., Markoulidakis J. G. and Theologou, M.E. (2009), Towards Anonymous Mobile Community services, *Journal of Network and Computer Applications*, 32 (2009) 116– 134.
6. De Hert, P., Gutwirth, S., Moscibroda, A., Wright, D., González Fuster G. (2009), Legal safeguards for privacy and data protection in ambient intelligence, *Pers Ubiquit Comput* (2009) 13:435–444.
7. Facebook (2009), About Facebook, retrieved August 2009, from http://lhup.facebook.com/about.php.
8. Felt, A., & Evans, D. (2007). *Privacy protection for social networking APIs*. http://www.cs.virginia.edu/felt/privacy/ retrieved 2009-08-25.
9. Fogel J. and Nehmad, E. (2009), Internet social network communities: Risk taking, trust, and privacy concerns, *Computers in Human Behavior*, 25 (2009) 153–160.
10. Guarda, P. and Zannone, N. (2009), Towards the development of privacy-aware systems, *Information and Software Technology,* 51 (2009) 337–350.

11. Guha, S., Tang, K. and Francis P. (2008), NOYB: Privacy in Online Social Networks, WOSN'08, August 18, 2008, Seattle, Washington, USA.

12. Hoadley, C.H., Xu, H., Lee, J.J., and Rosson, M.B. (2009), Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry, *Electronic Commerce Research and Applications*, accepted 04 May 2009.

13. Hosio, S., Kawsar, F., Riekki, J. and Nakajima T. (2007), DroPicks – A Tool for Collaborative Content Sharing Exploiting Everyday Artefacts, in H. Ichikawa et al. (Eds.): UCS 2007, LNCS 4836, pp. 258–265, 2007.

14. Hogg, T. (2009), Inferring preference correlations from social networks, Electronic Commerce Research and Applications, accepted 07 April 2009.

15. Kacimi, M., Ortolani, S. and Crispo, B., Anonymous Opinion Exchange over Untrusted Social Networks, SNS'09, March 31, 2009, Nuremberg, Germany.

16. Kalloniatis C., Kavakli E. and Gritzalis S., Addressing Privacy Requirements in System Design: the PriS Method, *Requirements Engineering* (2008) 13: 241–255.

17. Korolova, A., Motwani, R., Nabar, S. U., Xu, Y. (2008), Link Privacy in Social Networks, CIKM'08, October 26–30, 2008.

18. Krishnamurthy, B. and Wills, C. E. (2008), Characterizing Privacy in Online Social Networks, WOSN'08, August 18, 2008, Seattle, Washington, USA.

19. Larkin, E., Can Facebook Be Private? If You Care, Follow These Tips, Pc world.com**,** July 2009.

20. Lucas, M. and Borisov, N. (2008), FlyByNight: Mitigating the Privacy Risks of Social Networking, *WPES'08*, October 27, 2008, Alexandria, Virginia, USA.

21. McDonald, A.M.. Reeder, R.W., Kelley, P.G. and Cranor, L.F. (2009), A Comparative Study of Online Privacy Policies and Formats, in Goldberg and M. Atallah (Eds.): PETS 2009, LNCS 5672, pp. 37–55, 2009.

22. Miluzzo, E., Lane, N.D., Eisenman, S.B., and Campbell, A.B. (2007), CenceMe. .Injecting Sensing Presence into Social Networking Applications, G. Kortuem et al. (Eds.): EuroSSC 2007, LNCS 4793, pp. 1–28, 2007.

23. Pearson, S. (2009),Taking Account of Privacy when Designing Cloud Computing Services, *CLOUD'09*, May 23, 2009, Vancouver, Canada.

24. Pingel F. and Steinbrecher, S. (2008), Multilateral Secure Cross-Community Reputation Systems for Internet Communities, S.M. Furnell, S.K. Katsikas, and A. Lioy (Eds.): TrustBus 2008, LNCS 5185, pp. 69–78, 2008.

25. Raento, M. and Oulasvirta, A. (2008), Designing for privacy and self-presentation in social awareness, Pers Ubiquit Comput (2008) 12:527–542.

26. Ravichandran, R., Benisch, M., Kelley P.G. and Sadeh, N.M. (2009), Capturing Social Networking Privacy Preferences: Can Default Policies Help Alleviate Tradeoffs between Expressiveness and User Burden? In Goldberg and M. Atallah (Eds.): PETS 2009, LNCS 5672, pp. 1–18, 2009.

27. Weiss, S. (2009), Privacy threat model for data portability in social network applications, *International Journal of Information Management* 29 (2009) 249–254.

28. Wright, D., Gutwirth, S., Friedewald, M., De Hertb, P., Langheinrich, M and Moscibroda (2009), A., Privacy, trust and policy-making: Challenges and responses, *Computer Law & Security Review,* 25 (2009) 69–83.

29. Xu, H. (2009), Consumer responses to the introduction of privacy protection measures: an exploratory research framework, *International Journal of E-Business Research*, 5, 2, 2009, 21–47.

Applications to Improve Privacy on Online Social Networks

Víctor Rodríguez
Anna Carreras
Eva Rodríguez
Jaime Delgado

Universitat Politècnica de Catalunya

Abstract. Privacy management is different across the many online social networks and not always satisfies the user expectations. Some social networks members may demand choosing their privacy preferences more richly and exercise a tighter control on the information they drop. For this regard, it is under question if some of the Digital Rights Management systems features may be incorporated to the privacy management in social networks, and if the privacy terms themselves can be expressed in standardized policy languages, like XACML, additionally bringing interoperability across the networks.

Keywords. Privacy, social networks, information sharing.

1. Introduction

Online social networks are communities in the Internet, usually around one website, which connect users voluntarily sharing information. Information exchanged through online social networks cover a broad range of topics, ranging from simple personal information to the most bizarre contents.

In the last few years, social networks have been actually *the* Internet phenomenon, and the main axis of the so called Web 2.0. According to the web traffic ranking provided by Alexa, online social networks are among the most visited web pages in the Internet. For example, Facebook, MySpace, Hi5, Twitter or Orkut are in the 50 top pages in visits. Other topic-oriented social networks take good positions in the ranking too: LinkedIn, focused on professional profiles achieves a 96th in the ranking, Flickr for the photographs exchange, a 30th position and some dating and adult sites are also in this range; sharing essentially the features with generic-oriented networks.

These Internet sites are administered by *social network providers* who usually make (or try to make) profit of the network, even though users provide information for free. The income sources of social networks providers include advertisement in the web page, data mining, use data analysis and ultimately

exploitation of the contents themselves –the latter business model having been questioned.

Online social networks replicate to some extent the social relationships established in the ordinary life, with some particularities. The potential of computing and the spread of computer networks are not readily present to the users, who in the Internet experience tend to behave more carelessly and with less discretion. This has been proved in empirical experiments as in 0. In the most popular social networks millions of users add their personal profiles with the sole intention of communicating news about themselves and gossiping other's. However, and in the contrary as it happens in ordinary life, all the relationships pass through a single hub which knows –or has access to know– everything.

Thus, when speaking about privacy on online social networks we have to distinguish then two aspects: how to hide or limit the information visible to other peers (a concern also valid in ordinary social life) and how to control the use of the information that the social network provider will make (a concern peculiar of this world). For the first case, social network providers offer the user some configurable settings, in view of their customer's interest. For the latter case, social networks providers are limited by the law terms and excepting this, they currently use the information as they consider more convenient or profitable. The situation may progress to a state in which online social network users are also aware of this use and start valuing the privacy policies of the site. In this case the use of open standards and clear transactions may enhance the user's trust in the site and ultimately build customer loyalty to the social network provider.

Online social networks providers always give a privacy policy page in their sites, well visible and which has to be acknowledged by the users at least once at registering time. This web page is in all the cases a narrative expression which perhaps will evolve to standardized forms –just as CreativeCommons symbols replaced verbose texts in copyright statements in Internet resources. Currently the user expresses his privacy preferences by filling in forms (with radio buttons, check boxes etc.) in a configuration page of the web site. The presentation of these preferences and how the site internally represents them remains nowadays variable from social network to social network and far from any standard or pattern. Privacy policy statement actually looks like the transposition of a narrative contract clause from a text paper to a webpage. The authors of this paper envisage that this arrangement may change towards standardized forms. By doing so, the user experience will be improved, the joint use of different online social networks will be boosted and a minimum quality level will be achieved.

This paper is organized as follows. First, a detailed analysis of the current privacy policies used in social networks is presented in Section 2. Then, the different elements involved in a Digital Rights Management (DRM) system are introduced in Section 4; and a brief state-of-art in policy languages is presented in Section 3. Finally, Section 5 analyzes the use of DRM for specify-

ing privacy policies in Social Networks, and Section 6 presents two possible standard-based implementations of privacy applications, one based on a policy language, and the other based on a right expression language.

2. Privacy on online social networks

2.1. Privacy respecting the social network provider

There is a common set of privacy policies that everyone handling someone else´s personal data must implement: those defined in the law. The legal provisions vary slightly from country to country, but in general individuals are granted with similar rights: the right to rectify the given personal data, the right to be erased from the computer records of the provider´s database etc.

International companies handling personal information which want to operate in the European Union must adquire a certificate: TRUSTe certifies the compliance of the sites with the EU Directive on Data Protection 0. This Directive prohibits the transfer of European citizens' personal data to companies in foreign non-European Union nations unless they are certified. The TRUSTe seal grants that a site satisfies the seven *Safe Harbor Privacy Principles*, an agreed framework to qualify companies to share information across the borders. The Safe Harbor Privacy Principles constitute a good base to declare what is desired in the privacy prolicies to be implemented by the social network provider, and how can DRM or policy languages help. These principles can be seen in Table 1, as well as its degree of satisfaction by the social network providers.

Table 1. Safe Harbor Privacy Principles in social networks

Principle	Meaning	Satisfaction
Notice	Do social networks inform the users that their data is going to be collected and used?	Yes.
Choice	Do social networks offer to opt out the collection and forward transfer of the data to third parties?	Yes (at least in theory).
Onward Transfer	Do social networks grant that data transferred to third parties will only happen if these also follow adequate data protection principles?	Uncertain.
Security	Do social networks make efforts to prevent loss of collected information?	Yes, but these efforts are unclear.
Data Integrity	Is data used for the purpose it was collected for in the social networks?	Data is used for other purposes too.

Principle	Meaning	Satisfaction
Access	Can users access and delete the information social networks have on them?	Mostly.
Enforcement	Do social networks provide effective means to enforce the previous principles?	No.

In all of the social networks the principle of *notice* is satisfied: users have to actively declare that they know the privacy policies of the site. Most of them, too, satisfy the *choice* principle, by which they can restrict the data not to be leak to third parties, with a brief reference to how will data be handled after the *onward transfer*. And while it is true that *security* is a concern of social networks providers, there is no mechanism to grant this beyond some vague legal responsibilities. *Data integrity*, as described in Table 1 is in practice not respected at all, given that social network providers reserve themselves the right to use the given data as they consider more convenient. Users can *access* and rectify their data freely (on despite of the threat of Facebook of retaining the data for good). *Enforcement* comes only from the auditing offered by TRUSTe or similar certifying authorities.

The TRUSTe group has certified at least two of the major networks (Facebook and MySpace), who also suscribe other privacy initiatives, like the Children's Online Privacy Protection Act. Audit trails, monitoring and enforcement are granted by the TRUSTe seal, but in practice the control looks somewhat weak. Implementation of the seven Safe Harbor Privacy Principles is irregular, especially in what limits the social network provider data use. It has to be considered that with this paradigm, it is the social network provider the one who has to regulate himself. This commitment at least nominally was assumed in front of the European Commision recently, when a declaration of intentions was approved by some of the major social network providers in Europe[1].

2.2. Privacy respecting other users

Most of the online social networks providers have acknowledged the importance of the privacy policies and besides satisfying the legal requirements they offer their users some advanced configuration parameters going beyond the legal minimum. These extended privacy restrictions are of course offered to protect members from other members, but not from the social network provider themselves.

1. Safer Social Networking Principles for the EU, on Februay 2009. Site: http://ec.europa.eu /information_society/ activities/ sip/self_reg/social_netwk/index_en.htm

There is a common consensus around the idea that more control should be given to the users for the privacy matters in the Web 2.0 0, and it is likely that social network providers go deeper in this matter as long as it does not collide with their business model.

Current social networks allow users to specify who is able to access which pieces of their personal data. In the specification it is sometimes possible to declare which data is disclosed to all, to nobody, to the network contacts or to the contacts of the contacts. This specification can be clearly improved and refined. For example, data could be restricted in function of the age of the recipient user, or the sex, or the country etc. As it will be seen, standard policy languages could be used for this regard.

Open protocols are currently not followed, although a few of the sites allow the user to export their data as RDF (using FOAF, the Friend-Of-A-Friend vocabulary). Worldwide privacy policies standardization is still missing, but this would help the work of the social network owners in order to improve privacy. This good situation in theory is less perfect in practice, and there is still the need for new standardization initiatives easier to implement.

For example, the social network provider servers are secure in front of attacks for their own but none of them takes responsibility to grant their perfect functioning. Thus, each of these networks is liable to suffer virus attacks and data theft while no responsibility is taken at least according to the policy terms they publish, given that judges may say different.

Secondly, the execution of some user rights is not immediate and requires a human intervention which might delay fatally its effectiveness. Currently, millions of photographs are being uploaded daily, and in most of them some other people appear different from the person that is making the upload and of course has not been given any consent.

Thirdly, the terms of privacy also unanimously reflect the exceptions provided by governmental interventions, and for the most privacy paranoics it is not pleasant to be observed at discretion by governments

Some of these privacy flaws might have been avoided with mere technological measures. Information management strategies derived from those already existing in DRM systems may fix them. Thus, automatic complaint management and preventive deletion as default policy may have worked for some cases or data encryption might prevent state intromission in the citizens' private life. In the next sections, it will be seen how DRM systems and standard privacy policies can help to overcome some of the problems.

3. Policy languages

Policy languages are usually employed to control the access to resources, e.g. digital assets or applications. This is exactly what is demanded in online social networks, so it could be thought that expressing privacy preferences in one

standard policy language could allow having interoperability across the social networks and developing Web 2.0 applications in a standardized way. Are current languages operative enough as to serve for this purpose?

Some of the policy languages are the P3P (the Platform for Privacy Preferences 0), XACML (Extensible Access Control Markup Language 0) or the "Common Policy", specified in RFC4745 0 and which defines a framework for authorization policies controlling access to application-specific data. More recently, a W3C group is giving steps towards a new language integrating features of the three precedents (PLING, Policy Language Interest Group 0).

P3P enables web sites to express their privacy practices in a machine readable format that can be retrieved automatically and interpreted by other agents, like Internet Explorer or Mozilla Firefox. When visiting a P3P-enabled web page, the browser can understand the site´s privacy policies in a simplified and organized manner, and react accordingly to user preferences (for example regarding cookies etc.).

XACML is the language specified by OASIS 0. This standard policy language was devised for expressing authorization policies in XML, intended to be applied to any object that can be identified in XML.

The XACML standard specifies a policy language model. This model defines the rule element, which is used to define the set of resources, subjects, actions and environments to which the rule is intended to apply. In the rule element also it can be defined the consequence of a true evaluation for the rule, as well as the conditions to refine the applicability of the rule.

The XACML standard uses the W3C XML-Signature Syntax and Processing Standard 0 for providing authentication and integrity protection for XACML policies. The XACML version 2.0 specification provides the model descriptions for data-flow, XACML context (canonical representation of a decision request and an authorization decision), and policy language (rule, policy, policy set). However, in the last term, XACML does not define any rule per se, and this makes an hypotetical interoperability situation among different networks quite difficult to be achieved.

The IETF Common Policy actually defines a very simple XML Schema and expects that the different applications complete it through extensions.

Each of these policy languages looks appropiate to express the user preferences, but they particular profiles for social networks should be specified.

4. DRM systems

Current Digital Rights Management systems can manage digital assets in a controlled way, and according to the terms imposed by the content creators. Web-based social networks do certainly manage content –user generated content– but do not attain all the goals achieved by DRM systems.

DRM systems enable the creation, adaptation, distribution and consumption of multimedia content according to the permissions and constrains imposed by content creators and rights issuers –much as it should be in information released on social networks. There are different initiatives, standard and proprietary, that specify a DRM system or the elements that usually form these systems. Next subsections describe the elements that participate in a DRM system, compared to their counterparts in social network sites.

4.1. Digital objects

The digital objects creation process involves the combination of the protected digital assets with associated metadata to create digital objects that include the usage rules, information regarding the protection tools and other data as the creator of the asset, etc. User generated content in social networks does not differ from intellectual property protected content exchanged in DRM platforms, but tools to create content and to include usage rules are normally not provided.

4.2. Rights expressions

Rights expressions govern digital assets through the complete digital value chain in DRM systems. They are presented to the different actors of the value chain as XML files, usually called licenses, which are expressed according to a specific and rich Rights Expression Language (REL). Licenses also can hold protection information, such as the keys needed to decipher the digital content. Licenses are usually digitally signed to ensure the integrity and authenticity of their content, and sensitive data within them is usually encrypted. In social networks, users can, in the best case, specify which is the intended audience (none, all, friends, friends of a friend, etc.), but cannot normally express their restrictions with conditions as it is possible with a REL. Rights expression languages and policy languages do not differ much in vocation and form.

4.3. Rights enforcement

DRM systems have to guarantee that license terms governing digital assets are respected by the users of the digital value chain. For this reason, authorization tools are an important element of a DRM system. These license based authorization tools verify if a user has a license that grants him the right to perform the operation he is trying to exercise and if he fulfils the conditions specified within the license. In social networks, everything relies in the confidence the user has on the social network provider. His overall satisfaction of the enforcement is only vaguely granted by external audits.

4.4. Intellectual property protection tools

Different protection techniques are used by DRM systems. Usually, digital assets are protected using encryption and scrambling techniques, while other techniques as watermarking or fingerprinting are used for tracking or verification purposes. Usually, the information about the tools used to protect digital resources is associated to them in the digital objects creation process. Social networks do not provide protection tools, as this would detriment the provider´s interest of knowing everything what happens in the network.

4.5. Notification of events

Some participants of the distribution chain, as content creators or distributors, could want to monitor the usage of their copyrighted material. Therefore, some mechanisms will be necessary to allow systems to share information about events referred to multimedia content and peers that interact with the content. Social networks provide only residual information on events: it is not always possible to track who has seen a picture, but at least in some of them it is possible to know how many people have seen it.

4.6. DRM players

They consume digital objects according to the terms and conditions specified in the associated licenses. Then, DRM players make use of license based authorization tools that resolve if users are authorized to consume digital assets. If the user is authorized, then the content is deciphered and rendered. Typically, DRM players have a secure local repository for the storage of licenses, protection information, offline operations reports and other critical data. Nearly the only way of rendering user generated content in social networks is browsing the social network site. However, richer possibilities are open given that the APIs that these sites provide may eventually allow the construction of content players independent of the social network website. If enforcement techniques are to be applied, this could be integrated in a new site embedded player or in some software created through the available APIs.

5. DRM and personal data property rights

Online social networks have built their business models on the personal data that users freely share with others. This implies an increasing privacy risk on online social networking applications managing user's personal data. New privacy challenges and risks in the Web 2.0 have been studied in, and solutions DRM-based (see Section 3) have been already been explored like in 0, where a privacy schema extended the MPEG-21 REL vocabulary and resources were protected by IPMP tools within a security framework.

Sharing in online social networks means that users want to share data with other users. Currently, service providers make available collaborative tools to users for sharing data. However, in some cases, users cannot state the terms under which they want to share their data, for example only with a particular group of users and under certain conditions. In this scenario, privacy safeguarding measures need to associate usage rights to user's personal data to determine the conditions of use of this sensitive content. Current DRM technologies can help in providing this functionality, since licenses expressed according to a REL can be used to determine the terms and conditions under which user's data can be used by others. A license conveys to an entity the sanction to exercise a right against a resource, if the set of conditions previously specified within the license are fulfilled. In an online social network, users can use licenses to control the usage of their personal data and contents. Then, if Bob, a user of the social network, wants to share his contents only with some of his friends, he will be the issuer of the license. The principal to which rights are granted will be the friends that Bob has determined, the right of the license will be the view right, the resource for example the photos of Bob's last album.

On the other hand, privacy languages also can be used to specify the access rules to user's data (digital assets and personal data). Both, REL licenses, as well as policies can be used in social networks to control the access to users' data. Licenses can be used to govern digital resources and a broad range of rights and conditions can be stated by users by means of one of current RELs and associated to the corresponding resource. However, as they have not devised to control the access to user's data in social networks, probably an extension or profile should be defined for these applications, as done in other environments as the mobile one.

Sensitive personal data also needs to be protected, e.g. encrypted or access-controlled, to ensure that license terms are enforced. Another important component of DRM systems are the license based authorization tools, which prove if a user has the appropriate permissions to perform the operation they are requesting, i.e. an action against a digital resource. In an online social network, authorization tools will solve if the users of the network can view, edit, etc. personal data of other users of the social network.

Finally, event reporting techniques can help on the generation of personal data usage reports. Notification of events is an important part of a DRM system, since systems using event reporting mechanisms allow to content creators and distributors of multimedia content to be informed of the usage of the multimedia objects they have provided. By means of the chain of licenses defining the contractual relationships between the actors of the value chain, they could be informed of the use of the content that they have created, adapted, distributed, etc. Afterwards, users illegally distributing content could be prosecuted by means of these activity records. MPEG-21 Event Reporting 0 standard provides a standardized means for sharing information about events amongst peers and users. Such events are related to multimedia content and peers that interact with them. In an online social network, event reporting tools can help users to

monitor the usage of their personal data. In this way, they can determine if any other user of the network is using or distributing private data illegally.

6. Specifying privacy applications for online social networks

Most of the online social networks allow developers to create applications that permit users to share content. These applications can be used by other users of the network. In June 2007 Facebook opened a development platform for integrating new applications into this online social network. Facebook allows developers to program social applications, which have available a set of external libraries that enable the access to the functionalities that Facebook offers. These applications basically are web applications, which can be accessed from the Facebook portal. Nowadays, most of these applications are used by millions of people everyday.

Developers can build applications that run on Facebook and let users interact with other users. A user that builds a new application can invite one of his friends to use it, and if she accepts it, then she can use the application within the Facebook portal. The applications are executed in an external server, outside the Facebook environment. The unique direct connection is through libraries and APIs which provide a set of basic functions in the javascript programming language to access to Facebook users data, which includes personal data, photos, messages, etc.

In this context, we have considered the development of an application to control the access to users' data within the Facebook portal. This application will allow users to define more complex access rules to control the usage of their audiovisual material. In this way, it is expected to enrich the privacy concept in online social networks with new conditions of usage. Currently, users can only specify who can access to their personal data in terms of all/nobody, those who belong to groups, to the group of friends, to the group of "friends of my friends", etc. What we propose is the definition of more complex rules as for example "*only my workmates can see the Christmas Dinner photo album during this month*".

As outlined in the previous section, the implementation of this privacy application could be done based on policy languages, or using rights expression languages. Thus, in the following subsections, the specification of these two possible implementations is described.

6.1. Specifications for implementing privacy based on XACML

Specifically, we propose to use XACML, previously introduced in section 5, for expressing authorisation policies in social networks. This standard specifies a policy language model. The three top-level policy elements defined for this mo-

del are: rule, policy and policySet. The rule element is the basic unit of management within an XACML policy administration point. The main components of the rule element are: the target, effect and condition elements. The target element defines the set of resources, subjects, actions and environments to which the rule is intended to apply. The effect element indicates the consequence of a true evaluation for the rule. The condition element refines the applicability of the rule. The policy element consists of rule elements and mechanisms for combining the results of their evaluation. The obligations element specifies the actions that shall be performed in conjunction with the policy evaluation. Finally, the policySet element enables the combination of separate policies into a single policy.

In the developed application, users can specify and associate more complex access rules to their data, which can be later shared with other users according to the specified policies. One example of an access rule that can be defined using the proposed application is to permit the access to the Christmas Dinner's photo album only to her workmates during this month. In this way, if any other user that doesn't fulfil the specified conditions tries to access to one of the protected photos, the application will not grant him access.

Table 2. Example of a XACML policy to control the access to a digital resource

```
<Policy>
  <Description> Access control policy </Description>
  <Target/>
    <Rule RuleId="urn:oasis:names:tc:xacml:2.0:example:SR1"
Effect="Permit">
      <Description> Any of Alice workmates can view the Christmas
dinner photo album during this month </Description>
      <Target>
        <Subjects>
          <Subject>
            <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:rfc822Name-match">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string"> Alice
workmates group </AttributeValue>
            <SubjectAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
DataType="urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name"/>
            </SubjectMatch>
          </Subject>
        </Subjects>
        <Resources>
          <Resource>
            <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
```

```
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:example:
vc:schemas:</AttributeValue>
            <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:2.0:resource:target-namespace"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </ResourceMatch>
          <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:xpath-node-match">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">/vc:Christma
sDinner</AttributeValue>
              <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:xpath"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </ResourceMatch>
        </Resource>
      </Resources>
      <Actions>
        <Action>
          <ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">view</Attrib
uteValue>
            <ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </ActionMatch>
        </Action>
      </Actions>
    </Target>
  <!-- Only during the January 2010 -->    <Condition
FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-
greater-than-or-equal">
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-
one-and-only">
        <EnvironmentAttributeDesignator
DataType="http://www.w3.org/2001/XMLSchema#date"

AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-date"/>
      </Apply>
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#date">2010-01-
01</AttributeValue>
```

```
      </Apply>
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-
less-than-or-equal">
       <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-
one-and-only">
         <EnvironmentAttributeDesignator
DataType="http://www.w3.org/2001/XMLSchema#date"

AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-date"/>
       </Apply>
       <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#date">2010-01-
31</AttributeValue>
      </Apply>
    </Condition>
  </Rule>
</Policy>
```

6.2. Specifications for implementing privacy based on MPEG-21 REL

MPEG-21 REL is defined as a collection of three XML schemata, called the core schema (denoted by the XML namespace prefix "r"), the standard extension schema (prefix "sx"), and the multimedia extension schema (prefix "mx"). These schemata define the fundamental elements of the language, some widely-useful conditions, and elements useful in copyright protection applications, respectively. We present here a suitable privacy extension schema that could be used for implementing a privacy model for social networks (detailed in 0). The parameterization of this model is based on the following elements: "user role", "recipient", "context descriptor" (information that needs to be protected), "situation", and "precision". The elements of the proposed privacy extension will be denoted by the namespace prefix "px".

First of all, we need to identify the elements already contained in the MPEG-21 REL license that could be easily mapped to the parameters defined in the privacy model. For example, the user who wishes to protect his/her personal information can be easily identified as the MPEG-21 REL *Issuer* (responsible for specifying the privacy policies) while the recipient of the contextual information corresponds to the MPEG-21 REL *Principal* (responsible for exercising the right over some content). Finally, the MPEG-21 REL *Resource* could be used to express a single or even a set of sensitive contextual descriptors that need to be protected.

The most difficult part is to identify how to express the "situation" and the "precision" parameters. "Situation" combines contextual descriptors such as "location", "time", "usage", and "nearby people". We already know, from our previous work in the adaptation authorization 0, that we can include MPEG-21

Digital Item Adaptation (DIA) 0 descriptors inside the MPEG-21 REL *condition* field. MPEG-21 DIA includes the most complete schema for describing multimedia contextual information (user preferences, terminal characteristics, etc). Thus it would have sense to include "location", "time", "nearby people" as MPEG-21 DIA constraints in the *Allconditions* field of MPEG-21 licenses. Nevertheless, to the best of our knowledge, a suitable descriptor does not exist in MPEG-21 to map "usage". Our proposal is to include a "px:usage" element in the conditions field. Finally, the "precision" is expressed implicitly, and hence does not need a special element in MPEG-21 licenses. The issuer of the license is responsible for introducing a more or less detailed description of the context (in the resource field) associated to every principal. For example, the user can define that he allows his family to know that he is in a certain city, but protect the access to the precise geo-coordinates.

It is also relevant to note that MPEG-21 REL defines an element named "r:propertyProcessor" that allows to express groups of principals (users) through roles.

An example of our proposed license based on MPEG-21 REL to govern the use of contextual information is shown in Table 3. It allows the "Family members" to know the "location" of the "User" in order to fix a dinner in the following days.

Table 3. Example of a license based on MPEG-21 REL to govern the use of context

```
<r:license xmlns:xsi = http://www.w3.org/2001/XMLSchema -instance
xsi:schemaLocation="urn:mpeg:mpeg21:2003:01-DIA-NS DIA-2nd.xsd
urn:mpeg:mpeg21:2003:01-REL-R-NS rel-r.xsd
urn:mpeg:mpeg21:2003:01-REL-SX-NS rel-sx.xsd
urn:mpeg:mpeg21:2003:01-REL-MX-NS rel-mx.xsd  urn:visnet:privacy
drm-privacy-px.xsd"   xmlns:dsig=http://www.w3.org/2000/09/xmldsig#
xmlns:dia="urn:mpeg:mpeg21:2003:01-DIA-NS"
xmlns:mx="urn:mpeg:mpeg21:2003:01-REL-MX-NS"
xmlns:r="urn:mpeg:mpeg21:2003:01-REL-R-NS"
xmlns:sx="urn:mpeg:mpeg21:2003:01-REL-SX-NS"
xmlns:mpeg7="urn:mpeg:mpeg7:schema:2001"
xmlns:px="urn:visnet:privacy"
xsi:noNamespaceSchemaLocation="licenses.xsd">
 <r:grantGroup>
    <r:grant>
      <r:propertyPossessor>Familiy members</r:propertyPossessor> <!--
   Principal-->
      <mx:view/>   <!-- Right -->
      <mx:diReference>
        <mx:identifier>city</mx:identifier>
```

```
          <!--Resource-->
        </mx:diReference>
        <r:allConditions>
          <px:Usage>family dinner</px:Usage>
        </r:allConditions>
      </r:grant>
  </r:grantGroup>
    <r:issuer>
   <r:propertyPossessor>User</r:propertyPossessor>
    </r:issuer>
</r:license>
```

Furthermore, also to the best of our knowledge, there is no real implementation of a privacy protection system based on MPEG-21 REL.

7. Conclusions

This paper has presented relevant privacy issues in online social networks. Specifically, we have focused on privacy related to the data that users share on these networks taking into account both users' digital resources, e.g. pictures or videos, as well as users' personal data, e.g. contacts, personal information, etc.

First, privacy risks on online social networking applications managing user's personal data have been analysed. Then, we have studied if current DRM techniques are suitable for protecting users' data to finally conclude that some elements of a DRM system, as RELs or protection tools, can be used to protect user's privacy. Finally, we have specified two privacy applications in current social networks. These applications have been integrated in Facebook, since this network provides a development platform for integrating new applications.

Acknowledgments

This work has been partially supported by the Spanish government through the projects MCM-LC (TEC 2008-06692-C02-01) and Segur@ (Centre for the Development of Industrial Technology (CDTI), CENIT-2007 2004, under a subcontract with Safelayer Secure Communications).

References

1. Gross, R., Acquisti, A., Heinz, J. H.: Information revelation and privacy in online social networks. In: WPES '05: Proceedings of the 2005 ACM works-

hop on Privacy in the electronic society. ACM Press, New York, NY, USA, pp. 71-80 (2005)

2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ((EU Data Protection Directive). Authoritative text of the Directive can be found in the Official Journal of the European Communities of 23 November 1995 No. L 281 pp. 0031 -0050
3. Weiss, S.: The Need for a Paradigm Shift in Addressing Privacy Risks in Social Networking Applications. In IFIP International Federation for Information Processing, vol. 262, pp. 161–171. Springer Boston (2008).
4. O'Reilly, Tim.: What is Web 2.0? – Design Patterns and Business Models for the Next Generation of Software. The Web As Platform. O'Reilly Media Inc. (2005)
5. International Standards Organisation. Information technology – Multimedia Framework (MPEG-21) – Part 15: Event Reporting. ISO/IEC 21000-15:2006
6. Delgado, J., Rodríguez, E.: Digital Rights Management Technologies and Standards. In Interactive Multimedia Music Technologies, pages: 249-283, Information Science Reference, New York, USA (2007).
7. Sheppard, NP and Safavi-Naini, R.: Protecting Privacy with the MPEG-21 IPMP Framework. In 6th International Workshop on Privacy Enhancing Technologies, Cambridge, UK, June, (2006)
8. International Standards Organisation. Information technology – Multimedia Framework (MPEG-21) – Part 5: Rights Expression Language. ISO/IEC 21000-5:2004 (2004)
9. International Standards Organisation. Information technology – Multimedia Framework (MPEG-21) – Part 4: Intellectual Property Management and Protection Componenets. ISO/IEC 21000-4:2006 (2006)
10. OASIS, Organization for the Advancement of Structured Information Standards, online at http://www.oasis-open.org/home/index.php visited on August (2009)
11. Bowman, M., Debray, S. K., and Peterson, L. L. Reasoning about naming systems. ACM Trans. Program. Lang. Syst. 15, 5, 795-825. DOI http://doi.acm.org/10.1145/161468.161471. (1993)
12. Carreras, A., Delgado, J., Rodríguez, E., and Tous, R.: The Impact of Context Information on User Privacy in Social Networks. In IDT Series, vol.3, ISSN:2013-5017 (2009)
13. Carreras, A., Barbosa, V., Kodikara Arachchi, H., Dogan, S., Andrade, M. T., Delgado, J., Rodríguez, E., and Kondoz, A.M.: Context-aware and

DRM-enabled content adaptation platform for collaboration applications. To appear in IEEE Multimedia, 2009.

14. International Standards Organisation. Information Technology – Multimedia Framework (MPEG-21) – Part 7: Digital Item Adaptation. ISO/IEC 21000-7:2007 (2007)
15. T. Moses (Ed.): eXtensible Access Control Markup Language (XACML) Version 2.0, Feb. 2005 http://docs.oasis-open.org/xacml/2.0/access control- xacml-2.0-core-spec-os.pdf (2005)
16. Eastlake D. et al.: XML Signature Syntax and Processing, W3C Recommendation, June (2008)
17. Cranor L. et al., eds, The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, W3C Recommendation, (2002).
18. Schulzrinne H. et al., eds, RFC 4745, Common Policy: A Document Format for Expressing Privacy Preferences. (2007)
19. W3C Policy Languages Interest Group, online at http://www.w3.org/Policy/pling/wiki/Main_Page visited August (2009).

Privacy Features of Authentication Systems

J. Herranz
[o]Departament de Matemàtica Aplicada IV, Universitat Politècnica de Catalunya

H. Pujol
J. Iñigo
*Safelayer Secure Communications, S.A.

Abstract. The wide variety of online services that appear every day offers new scenarios where privacy of citizens is concerned. In many cases, there are two apparently contradictory goals when dealing with the access to an online service. On the one hand, security of the service must be ensured, meaning that non-authorized users will not gain access to the service. On the other hand, the personal information that a user discloses when he requests access to the service must be minimal. In the last years, some authentication systems offering different levels of privacy and anonymity have been proposed. In this paper we review the state of the art in this area. We describe a very generic and common architecture for these systems, we list different (privacy) properties that authentication systems may provide, and we discuss which of these properties are satisfied by some of the existing systems.

Keywords: digital authentication, anonymity, authorisation, cryptography, privacy, web 2.0.

1. Introduction

An identity is made up of a number of roles that a subject may play in different social contexts. When the subject interacts, he shows a different profile to each audience, trying to reduce the disclosed information to a minimum, as well as keeping audiences apart. In general, users don't feel comfortable when they are asked to reveal their identity attributes beyond the limits of each context, and that is even more critical for their digital profiles, since digital information is easily stored, shared and processed.

Privacy Enhancing Technologies is a general term for a range of different mechanisms that protect sensitive personal data within information systems. Although users must be enforced to protect their digital identity and their activity trace in the Web, service providers must also be able to verify user's

legitimacy to access their services. This compromise leads to different authentication schemes that can provide a wide range of privacy features whilst they ensure enough security conditions.

The first solutions appeared when web applications and online services expanded and evolved: service providers generally opted to collect and manage users' information on their own, usually for business purposes. Such solutions are not fully satisfactory, because identity information is duplicated and dispersed in a large number of proprietary repositories, whereas only a subset of all the collected personal information is actually essential in order to provide each service.

Identity federation architectures try to solve this data dispersion problem, as service providers delegate the storage and management of all the personal identifiable information to an identity provider. In some of these schemes, like Liberty Alliance (Liberty, 2009), the identity provider takes part in every authentication process and therefore is able to trace the user activity completely. Other proposals like Information Cards (Burton, 2009), Idemix (Idemix, 2009) or U-Prove (U-Prove, 2009) pretend to involve the user in the personal data revelation process, empowering him to precisely state which data must be sent to the service provider.

The goal of this paper is to give a general view of how these architectures for authentication with privacy work. In Section 2 we describe the Identity Metasystem Architecture (Identity Metasystem, 2009), and the different participants that take part in it. In Section 3 we review some common Web 2.0 scenarios that entail different security and privacy requirements. We list in Section 4 a set of features that anonymous authentication systems may provide, and we discuss which of them are provided by some existing systems. Finally, the conclusions of this work can be found in Section 5.

2. The Identity Metasystem Architecture

An Identity Metasystem defines a generic architecture where several identification schemes may interoperate. Identification schemes are based on digital identities, which are sets of claims or assertions made by one party about another party; these collections of claims are exchanged among parties in secure tokens.

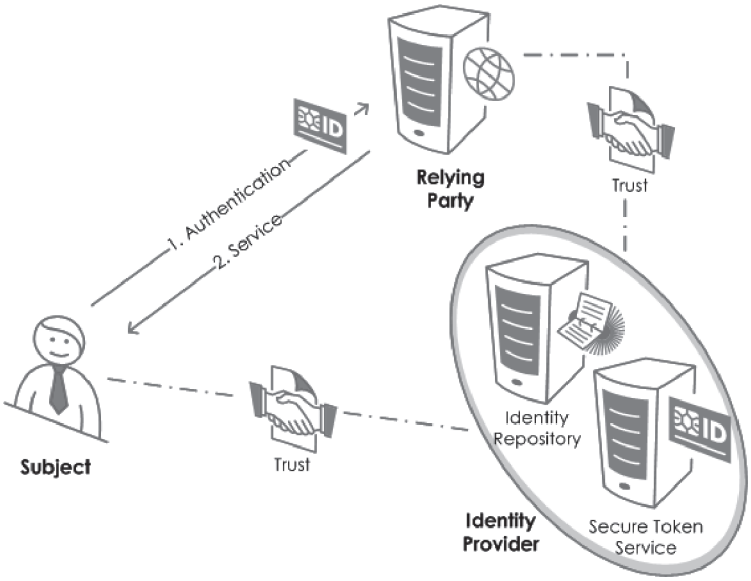
The three main participant roles in an identity metasystem generic architecture are:

- the Relying Party (or Service Provider), which is the network entity that provides the desired service, and relies upon a set of claims;
- the Identity Provider, which is the network entity that provides to each subject the digital identity claims used by a relying party;

– the Subject (or User), i.e. the individual or entity about whom claims are made by an identity provider.

In order for this architecture to succeed, two trust relationships must be established off-line. The first one between the user and the identity provider, as the identity provider is aware of and manages the user's identity information, and issues identity claims about him for identification, authentication and authorisation purposes afterwards. Another trust relationship must be established between the identity provider and the relying party, since the relying party trusts the information contained in secure tokens in order to provide a service or not, as long the secure token origin and integrity can be verified.

Figure 1. Identity Metasystem generic architecture.



Many different solutions –like Information Cards, Public Key Infrastructure, OpenID (OpenID, 2009), Idemix or U-Prove– fit such a generic architecture. Other authentication systems, like the one based on Traceable Anonymous Certificates (TAC, for short) (Park, 2008), fit a very similar architecture: in TAC-based solutions, the role of the identity provider is actually played by two entities, a blind issuer (BI) and an anonymous issuer (AI).

According to the authentication scheme and the secure tokens format, different privacy features can be achieved, and therefore, different authentication systems may be used depending on the user's and the relying party's privacy requirements.

Therefore, privacy requirements should be identified and taken into account from the very beginning of an information system design process, as

recommended by the Laws of Identity (Cameron, 2005). In fact, the following two basic questions should be answered:

1. What is the minimum necessary personal information needed by a relying party so as to provide a service?
2. In case an authorised third party requires the disclosure of the authentication session information, is there any legal obligation for any of the parties to handle and store any particular identity claim?

The answers to those two questions could determine whether a complete anonymous authentication scheme would be appropriate, or a more privacy-invasive system should be deployed in each use case.

3. Use Cases

Web 2.0 is built upon a wide variety of collaborative services and applications that must take into account user's privacy preferences from the design phase. Some interesting design principles may be found in (Koorn, 2004), in particular, those concerning personal data protection in information systems. Functional requirements should state whether the processing of personal data for authorisation purposes is a) essential, b) essential to a limited extent, or c) avoidable. Depending on the case, an appropriate identification and authentication mechanism could be selected, since they all have different properties.

3.1. E-Governance

According to the European Commission, e-Governance is about using the tools and systems made possible by Information and Communication Technologies, like Web 2.0 applications, to provide better public services to citizens and businesses. It encourages citizen participation, also known as e-Democracy, to involve them more directly in the decision processes, not only in popular consultations (which are a particular case of e-voting), but also in opinion polls and electronic suggestion boxes. For example, Barcelona City Council is currently promoting citizen participation in the remodelling of the Diagonal Avenue, and has started a campaign for citizens to propose ideas and give their opinion about how this communication axis should be in the future.

Unlike e-Voting, e-Governance processes may be ruled by ad hoc regulation. The surveying entity may ask citizens to demonstrate certain characteristics like, for example, being over 16, being registered in a certain census, or to work in a certain corporate sector. Moreover, entitled citizens may participate only once or as many times as they like, and they may be able to choose whether to reveal their identity or not. All these prerequisites will determine which identification authentication and authorisation mechanisms should be adopted.

3.2. Social applications

Users keep building up their digital identity every time they contribute to social applications with posts, comments or tags among other digital contents. Therefore, as they keep leaving public traces of their personal and professional activity, they should be able to control more closely which personal information they reveal.

So far, anonymous web browsing techniques have allowed hiding the actual user's IP from service providers. However, access control is usually performed at an application level, so users must still provide their identification information and authenticate at the service provider. But actually, some collaborative applications like forums and tagging tools don't really require a user complete identification, as the authorization process could be based on features like seniority, experience or reputation. Then, only a few sets of identity attributes would be necessary and pseudonym authentication could be used.

In the social networks case, the self-registration procedure and the self-managed privacy preferences allow the users to control their privacy to some extent. But this poses a basic trust dilemma: the user is supposed to accept a statement of responsibilities when he signs up, and the service provider assumes, for example, that the user is not under a certain age.

In order not to leave this responsibility to the users only, and with the aim of protecting particularly vulnerable groups like children, more rigorous authentication procedures should be adopted, whilst privacy control and self-registration should remain possible. Then, users should have the means (and should be required) to prove a minimum subset of their identity attributes (for instance, "I am over 13"), but still be able to fill in the rest of their identity information on their own responsibility.

3.3. E-Commerce and digital contents distribution

Internet is already widely accepted as a global marketplace. Physical goods and digital contents are sold, and the Network itself has become a regular distribution platform for software, music and computer games industry. As e-commerce entails some particular requirements –like the service provider being able to verify that the payment has been correctly made, and being able to deliver the purchased assets– many electronic payment schemes have been developed so far (for example, bank proprietary payment gateways or PayPal).

These schemes focus on guaranteeing the authenticity of the three-way transaction, and ensuring that certain critical compulsory attributes remain hidden (i.e. like the bank account details). All through the acquisition process, the customer should be able to protect his privacy in front of the service provider (as it is not always necessary that the service provider knows who the buyer is) and in front of the payment service provider (as the latter shouldn't be able to know what the customer is buying).

4. Anonymous Authentication Properties

The formerly described scenarios point out different requirements for authentication processes. According to these requirements, some particular features will be expected from an authentication system. This section describes a collection of properties that authentication systems may have, particularly concerning user's privacy. We briefly discuss which of these properties are achieved by some existing authentication systems: digital certificates, OpenID, Information Cards, Traceable Anonymous Certificates (TAC), U-Prove and Idemix.

4.1. Anonymity

One of the main goals of privacy-preserving authentication is to protect user's anonymity, by preventing the capacity of relating his real identity with the interactions he has with the different relying parties. A clear example of authentication system that does not provide any anonymity is the usual PKI framework: digital certificates explicitly associate a cryptographic public key to the subscriber's identity. Therefore, each interaction of a user with a relying party, which implies showing his digital certificate, identifies this user univocally.

Other authentication systems offer different levels of anonymity. In most of them, anonymity cannot be complete, because system administrators always want to have a way of identifying users who break the law, for example.

In solutions like OpenID and Information Cards, the identity provider is the only who can link a user interaction with his real identity. In TAC-based solutions, it is required that the two entities that play the role of identity providers (blind issuer and anonymous issuer) agree and cooperate to identify a user from an interaction with a relying party. Finally, both Idemix and U-Prove offer complete anonymity even in front of the identity provider, in their basic versions. However, they admit extensions so that an external entity (for example, a judge) can always extract the identity of a user from an interaction with a relying party, in case of misuse.

4.2. Unlinkability

Another important goal of anonymous authentication may be to prevent the capacity of linking different authentication sessions of the same user. Such a linkage is obvious and immediate in some cases. For example, a digital certificate immediately identifies the user who holds it, so any solution based on digital certificates can never provide any kind of unlinkability.

Other authentication schemes separate the identity provision from the service provision, thus offering a range of possible (un)linkability levels. For example, it may be (im)possible: a) to link different Alice's authentication ses-

sions at different service providers, or b) to link different Alice's authentication sessions at the same service provider. The following Table I summarizes the former features for our selection of authentication systems. RP stands for Relying Party, IdP stands for Identity Provider, and authN stands for 'authentication'.

Table I. Required roles in order to…

	…link different Alice's authentication sessions at *different* RP's	…link different Alice's authentication sessions at *the same* RP
Digital Certificates	Several RP are able to jointly link different Alice's authN sessions.	Always possible for the RP and for the IdP (if the certificate is publicly shown).
OpenID	Several RP are able to jointly link different Alice's authN sessions. The IdP is able as well, because it establishes a direct communication with the RP in each authN session.	Both the IdP and the RP are independently able to link different Alice's authN sessions at the RP.
Information Cards	Several RP are able to jointly link different Alice's authN sessions.	An RP is independently able to link different Alice's authN sessions.
TAC	Several RP are able to jointly link different Alice's authN sessions.	An RP is independently able to link different Alice's authN sessions.
U-Prove	Several RP are able to jointly link different Alice's authN sessions (only if the same token is used).	An RP is independently able to link different Alice's authN sessions (only if the same token is used).
Idemix	No one can link different Alice's authN sessions.	No one can link different Alice's authN sessions.

Unlinkability, when it exists, relies essentially on cryptographic techniques, on the user and session identifiers format, and on the security tokens exchange protocol. Note that in the case of U-Prove, linkability is possible only when the user employs the same token in two different authentication systems. Since in this system a user has one token for each attribute, it is believed that he will use the same token only when interacting with the same kind of Relying Par-

ties. For example, a token for a driving licence will be used when interacting with a company for renting cars, but now when interacting with an e-commerce site. If disjoint subsets of tokens are involved in two interactions of the same user (either with the same or with different relying parties) then no one can link these actions.

4.3. Required online roles

The identity metasystem architecture considers the participation of three roles –the subject, the identity provider and the service provider–, which interact basically on two particular occasions: during the identity information registration process and during the authentication process.

The identity information registration process involves mainly the subject and the identity provider, and usually, both parties will be required to be online during the course of the procedure.

On the other hand, the authentication process is triggered when the subject requests a service. In that case, different schemes may apply, and different combinations of online required parties may take place. For example, the service provider may need to establish a direct dialogue with the identity provider in order to verify user's identity (as in OpenID); this dialogue may be orchestrated by the subject (as in the Information Cards approach, where the service provider and the identity provider do not exchange information directly). Finally, in the rest of solutions considered here, the subject already holds a set of (certified) identity claims, like a digital certificate or a token, the service provider may verify on its own, without the participation of the identity provider.

Note that systems requiring more roles to be online will suffer from more communication latency, which results in less efficiency in practice.

4.4. Management of attributes

A digital identity is a set of claims, i.e. a collection of attributes and their corresponding values regarding a particular subject. The management of attributes and their life cycle also characterises authentication systems.

Some authentication mechanisms, like digital certificates, link the whole digital identity to a public key. Thus, when Alice authenticates at a service provider through her digital certificate, the service provider gets access to the whole of Alice's personal information contained in the certificate.

Other solutions enable the selective disclosure of attributes: Alice can specify which attributes she sends to the service provider (as in Information Cards).

Some authentication systems like U-Prove or Idemix are able to apply certain logical and mathematical operators on certified attributes. Thus, the user Alice can prove to the relying party, for example, that she is over 18 and that

she has more than 1,000 $ in her account, without disclosing at any point her exact age or the exact amount of money she has.

Finally, the claims that were made and certified by the identity provider may have a predetermined lifetime, or they may be revoked by an authorised third party.

4.5. Security and prevention of misuse

Privacy preservation must not have an effect on the security level of authentication systems, as subsequent critical authorisation decisions may rely on them.

Therefore, similar criteria must be taken into account in order to guarantee a required level of assurance, which refers mainly to the way how identity providers establish the identity of the end user (such as user and password, digital certificates, biometrics, etc.), and how securely user's credentials are stored (for example, as an encrypted file in the PC or in a PIN-protected smartcard). In addition, security will be reinforced by non-repudiation capabilities, as privacy-preserving authentication intends, by definition, to detach digital identities from their corresponding entities.

On the other hand, secure privacy-preserving authentication mechanisms should provide the means to hinder several kinds of attack like eavesdropping, as identity attributes should be protected from unauthorised verifiers, and spoofing, as a third party should not be able to impersonate another entity. Finally, some authentication mechanisms, like U-Prove, may dissuade unaware users from sharing their credentials as personal attributes are revealed after a certain number of uses.

4.6. Computational cost

The computational cost of cryptographic operations is also significant in authentication systems, during both the credential generation and verification processes.

A time-consuming credential generation or verification procedure may be critical when it takes place during the course of the authentication process, as they may delay the access to the service. Therefore, performance capabilities of hardware and software platforms employed by each one of the participant roles must be in accordance with the involved cryptographic algorithms. Algorithm selection shall also determine which platforms might be used (and vice versa), as regular commercial user hardware (whether it is a smartcard or a handheld device) is not yet ready to support the newest algorithms which use shorter keys for an equivalent security level, like those based on elliptic and hyperelliptic curves.

5. Conclusions and Future Work

As privacy observance is essential in many scenarios ranging from popular Web 2.0 collaborative tools to e-Governance and e-commerce, Privacy Enhancing Technologies should be taken into account from the beginning of the applications design process.

The identity metasystem architecture detaches the identity provision from the service provision, and defines the three main roles that play a part in authentication processes: the subject, the identity provider and the relying party. This architecture is appropriate for user-centric platforms, where user gains control of his privacy, is always aware of the amount of identity information that is revealed to other parties, and is even able to decide to what extent he wants to share this information with service providers.

Authentication schemes provide a range of privacy levels, according to their properties. In particular, the number of roles that are involved during the authentication procedure, and the exchanged identifiers format, will determine significantly the capacity of tracking user's digital activity. Anonymous authentication mechanisms, however, must still remain secure enough and allow the relying parties to verify user's legitimacy in order to authorise him to access the service.

This article lays the foundations to continue working on privacy-preserving authentication and authorization mechanisms, and to determine to which extent it will be possible to combine them with governmental initiatives like the European Citizen Card (Naumann, 2008 and 2009).

Acknowledgements

This research has been partially supported by Safelayer Secure Communications and the Centre for the Development of Industrial Technology (CDTI) of Spain, within the framework of the Segur@ project, reference CENIT-2007 2004 of the CENIT Programme, part of the INGENIO 2010 initiative (Segur@, 2009). Moreover, it consolidates a new research line, focused on the evolution of authentication technologies.

References

1. Liberty (2009), *The Liberty Alliance*, available at: http://www.projectliberty.org/ (accessed 14 July 2009)
2. Identity Metasystem (2009), *Identity Metasystem Interoperability Version 1.0* at: http://docs.oasis-open.org/imi/identity/v1.0/identity.html (accessed 3 August 2009)

3. Burton, C. (2009), *The Information Card Ecosystem: The Fundamental Leap from Cookies & Passwords to Cards & Selectors*, Information Card Foundation, April.

4. Cameron, K. (2005), *The Laws of Identity*, Microsoft Corporation, available at: http://www.identityblog.com/stories/2004/12/09/thelaws.html (accessed 20 July 2009).

5. Idemix (2009), *Idemix: pseudonymity for e-transactions*, available at: http://www.zurich.ibm.com/security/idemix/ (accessed 2 August 2009)

6. Koorn, R. et al. (2004), *Privacy-Enhancing Technologies. White Paper for Decision-Makers*, Directorate of Public Sector Innovation and Information Policy, Dutch Ministry of the Interior and Kingdom Relations, the Netherlands, December.

7. Naumann, I. and Hogben, G. (2009), *Privacy Features of European eID Card Specifications. Position Paper*, European Network and Information Security Agency (ENISA), February.

8. Naumann, I. and Hogben, G. (2008), *Privacy Features of European eID Card Specifications*, European Network and Information Security Agency (ENISA), August.

9. OpenID (2009), *OpenID*, available at: http://openid.net/ (accessed 2 August 2009)

10. Park, S. et al. (2008), *Traceable Anonymous Certificate*, Draft IETC, available at: http://tools.ietf.org/id/draft-ietf-pkix-tac-01.txt

11. Segur@ (2009), *Proyecto CENIT SEGUR@ Seguridad y Confianza en la Sociedad de la Información*, available at: http://www.cenitsegura.com (accessed 10 August 2009).

12. U-Prove (2009), *U-Prove Technology*, available at: http://www.credentica.com/technology.html (accessed 23 July 2009).

Section Two
Free speech and Web 2.0

Dissemination of information under neutrality principle in Spain[1]

Carles Alonso

Doctorate student (Universitat de Barcelona), Law assistant (Agència Catalana de Certificació)

Abstract. This paper analyzes some legal problems on dissemination of information in web 2.0 age. The Internet revolution is made of a bigger horizontality of relationships; we'll analyze if legal framework is ready to such radical changes on public communication sphere with the help of neutrality principle; besides, economic issues can be another legal element that's mixed with other elements, like freedom information or expression. That analysis will take 2 fundamental legal topics: legal acts and judicial policy. We'll try to clarify the legal past and future challenges with the aim to contribute to a wider and richer debate.

Keywords: dissemination, information, horizontalization, neutrality, revolution

1. Dissemination of information in the web age

The most important challenge on Information Society is the Copernican change of positions between actors for the dissemination of information. Before the web explosion, the information dissemination was generally made on vertical schemes: mass media, editorial market, cultural industries, among others, controlled the spread of information. The web age is the evidence to analyze the main effect of the digital revolution: the horizontality of the information relationships.

Web 2.0, wiki, formal or informal social networks, video and audio streaming, dialogue forums, discussion groups, All of these instruments or activities are the basis for a new political process, wider than ever before. Open scenarios for a more democratic expression of political opinions are different depending on the political regime. As Lawrence Lessig said (Lessig, 2002), the Internet is uncontrolled at macro levels, may it could be controlled at micro levels. Boas

1. This paper can be considered a largest explanation of some explanations made at alonso, Carles. La información en la Red y el principio de neutralidad tecnológica: la libertad de expresión y la difusión de información administrativa. Revista Vasca de Administración pública, nº 81/2008. Here I strictly study the dissemination of information by particulars.

(2006) showed us some examples for such possibilities of information control, even on authoritarian countries, and the different existent models of censorship (Chinese censorship –or privatized censorship–, Arabian censorship –centralized State censorship). On the other hand, the flexibility at macro levels can help the spread of information and makes effective political expressions.

As well, in the Spanish case, problems are similar to the ones in other states. We are convinced that the social interaction is much open, and I'll try to show with the help of different tools (judicial cases, social interaction, judicial and academic doctrine), the past and future problems that we'll see over the next years.

To properly analyze this matter, I will present the neutrality principle as a whole principle on technology law topics. Neutrality principle brings us a new vision of competition law as well (telecommunications, technology markets, architectural issues, etc.), but much more than this: due to the neutrality principle we can analyze the broadcasting law, criminal law, civil law...

2. Neutrality principle presentation

2.1. Neutrality principle general concept

The description of neutrality principle that I propose is taken from basic law principles. The technology progress introduces a few significant changes on different activities, so sometimes the fact fixed on legal text does not apply anymore. If the activity is already identified on all the elements of a legal text, the analogy can be used for resolving some cases, e.g. on theft cases (or others, see the examples in Lessig, 2002 –e.g. James Baker prosecution). But the majority of activities changed their elements because technology users wanted to do new activities or to bring new functions to communication tools.

The new possibilities overpass the existent legal framework and then the legal operator has to look for new solutions (usually on a parliamentary or a government act, but not always). These new solutions are conditioned by legal principles and the characteristics of new technologies. At a legal level, and in the Spanish case, the legal solutions can be more or less intensive, depending on the case. In the case of fundamental rights, the solution of neutrality principle is simply occupied by fundamental rights or liberties and their doctrine interpretation as well (this argument can be found in Sunstein, 2001, where he warns that economic activities are supported by classical freedoms).

In other cases, the use of technology has to be authorized: that's the case on administrative (public bodies) activities. The Spanish Administration is governed by the legality principle (the section 45 of the procedure Act was modified to legally sustain the use of new technologies. Now an entire Act –11/2007– is dedicated exclusively to 'citizen's electronic access to public services'. Some of the changes introduced are in line of the new technologies possibilities (e.g.

self-verification of documents, section 32.5 –"autocompulsa"–, the new duties for sharing documents, section 6.2.b).

The debate on neutrality principle has 2 main scenarios: the competition law and the peer-to-peer applications. On the first scenario, the 500.000 € fine imposed by European Community (EC) Commission to Microsoft is one of the most popular cases and examples. The discussion of Spanish electronic access Act was exclusively fixed on competition terms, because the captivity of Administration can disturb the competition conditions (affecting citizen's technological choices),[2] while neutrality principles is larger than this, both in private or public activities.

The P2P debates are actually debates about the definition of private copy and its legal regime. In Spain the solution was to copy the same rules adopted for VHS and cassette tapes (the compensation of alien intellectual property rights on a private basis), but this solution is not really neutral because the technological devices can store intellectual property rights protected files or other type of files (proper information as documents, pictures, public domain information, judicial decisions,[3] ...), as a difference from the analogical devices common use.

Lessig thesis (Lessig, 2004) is probably the best definition of neutrality principle: the technology can change radically some legal concepts; he shows analogically that thesis with the Causby's farm case. A military airport disturbed the animals (which hurt themselves running against the walls because of the noisy planes over them). Therefore, the Causby family prosecuted the military aerial activities arguing the classic definition of property that came up "to heaven". Judges expressed the negative response with such a sentence "[The] doctrine has no place in the modern world. The air is a public highway, as Congress has declared. Were that not true, every transcontinental flight would subject the operator to countless trespass suits. Common sense revolts at the idea". Our conclusion, with Lessig, is that law changes because an adjustment is made to the new possibilities of technology. Lessig speak about the common law system, but this is an example of changes on legal –and social– norms in democratic societies. So, technology specialities will impose themselves, because legal norms that think on past technologies will provoke the revolt of common sense.

Finally, the neutrality principle can be defined both in a vertical and in a horizontal sense. Lessig (2006) describes those 2 faces of neutrality principle with the example of Pics technology, because Pics can be used to filter some us-

2. See the first regulation of administrative services in France (Section 2.1.2, Circulaire du 7 octobre 1999 relative aux sites internet des services et des établissements publics de l'Etat).

3. There is a diversity of judicial cases about that tax-exoneration for judicial decisions (all of them already closed): Sentencia de 15 de junio de 2005, del Juzgado de Primera Instancia nº 7, de Alcalá de Henares, Sentencia de 14 de diciembre de 2005, del Juzgado de Primera Instancia nº 43, de Madrid, Sentencia de la Audiencia Provincial de Málaga de 19 de septiembre de 2006 y Sentencia de 2 de febrero de 2006 del Juzgado de lo Mercantil nº 5 de Madrid

ers (e.g. a server on a country where gaming is legal can exclude citizens from a country where gaming is illegal) or some contents (a particular can filter some information –e.g. the enterprises filter some contents to their workers, parents can filter some contents, ...).

In the following sections we'll know how the neutrality principle is present in new legislation referring various sectors of activities.

2.2. Neutrality principle on broadcasting activities

Neutrality principle is present in broadcasting services legal framework. In Spain, autonomous communities can legislate and execute their own Law,[4] while it exists a EC-level global regulation for economic topics and a State-level law for state-level televisions,[5] radios and telecommunications activities (cable, satellite TV are regulated in state acts but some functions can be developed by autonomous communities). I'll explain the Catalonian legislative acts only in an aim to visualize the given concept, in coordination with EC directive.

Neutrality principle is focused on the indifference for the technology employed: the broadcasting material law applies to communication services independently the technology used [the technology used by producers is only relevant on the beginning of activities regime, so an Internet communication service doesn't need an authorisation because the Internet resources are not a public and limited space]. The analogical televisions and radios –and DVB services, commonly called TDT– have to obtain an authorisation delivered by an Independent Administration, the Catalonian Broadcasting Council,[6] as a condition to begin the activities (excluding community services that had a different regime).

The concept of communication services is adopted in line of the new Directive (recently reformed 2007/65/EC), even the Catalan act was adopted before the new directive, because some concepts were already adjusted to the new technologies; otherwise, internal broadcasting law should be interpreted in conformity of the directive. The idea of communication service includes electronic communications, lineal and non-lineal activities as defined in the text and in the preliminary text of the directive. A communication broadcasting media is a service: 1) responsible for the contents (there are not third parts or a community of different producers), 2) whole dedicated to such activity to inform, educate and entertain (the broadcasting activity is the principal goal

4. Autonomous Communities in Spain are similar to member states on a federal schema; they have legislative and executive powers.

5. Probably, that's an irregular application of Constitutional distribution of powers, but this subject so far away from our matter, see Fernández Farreres, 1997.

6. See sections 16 and 60.1 of the Catalunya Audiovisual Communications Act (Llei –Parlament de Catalunya– 25/2002)

of the organisation, and it is not incidental activity), 3) with a commercial orientation/goal.[7]

Therefore, we can conclude that dissemination of broadcasting products on the Net can be or not subjected to broadcasting law or not, depending on the activity itself. So, it does easy differentiate professional activities and the non-professional or non-commercial activities.

Other activities can be object of law depending on some cases: these can be commercial activities, so the law of publicity or commercial offer can be applied; the broadcasting activities for citizens exercise of expression or information freedom cannot be object of broadcasting law but some principles referring the definition of the citizen rights and artistic expression (remember the Decency Communications Act decision of USA Supreme Court and its references to James Joyce's Ulysses).

Finally, for other activities a new legal regime can be made. For an example, an institutional broadcasting activity (e.g. for diffusion of the representative chambers sessions) will need a new law adapted to the characteristics of the new technologies and respecting the principles of public administration, because the administrative services of the chambers are the producers and diffusers of information (see ALONSO, 2008), so the legal space to be applied to such activities is not the chamber-functioning regime, but the public services regime.

Neutrality principle help us find the legal space to some activity on analyzing the main characteristics of activity (in this case, the activity is made by administrative services of chamber and has to be objective (in our case, Public Administration serves the general interest "with objectivity", see section 103 of Spanish Constitution); so, new legal framework can be made to protect citizens of an unfair use of technologies (to protect citizens position from the main political groups, which can use the administrative services for their own profit), and adapt that use to technology possibilities (preservation conditions, identification of institutional broadcasters with signature technologies, etc).

2.3. Neutrality principle on information society services

2.3.1. Information Services legal framework

Information Society Services law is the result of European Communities authorities doubts about the electronic commerce developing.[8] The aim of the resultant Directive was principally to facilitate the European market conditions to the technological companies (e.g. as servers renting) and some indications of electronic commerce providers (the 2-steps shopping, really is a civil

7. See 18 and 19 of 2007/65/EC Directive

8. In fact, the neutrality principle appeared the first time at the UNCITRAL Model Law on Electronic Commerce

law problem –the effective voluntary shopping). The only norm about contents was the liability premises, so the only responsible is the person or organization who effectively knows the contents of the servers. In conclusion, the directive is addressed to economic service (and remarks when said "normally provided for remuneration").

A very important element of European law is its power limitation, because European law is a market law, but not a constitutional law (with some developments as the fundamental rights bill). So, the rest of the legal framework (e.g. law for contents) is an internal powers matter. Here rise up the first problem for 2 reasons: 1) because Spanish legislator usually copy & paste the content of EC directives, 2) because the Spanish legislator and legal operators don't understand the scope of some legal concepts.

In fact the section 8 of Spanish act rules the erasing or retiring contents by authorities, and the debates are always focused on the "competent authority" (administrative and/or judicial authorities), because the directive didn't point that question (because European community doesn't have power to rule these matters).

Freedom of expression, personal or European contents should be analyzed from an internal law point of view (commercial law for commercial information, constitutional law for freedom of expression or others...), because EC law (and internal law) should be neutral. It's clear that some contents can be object of a administrative powers in some cases, but it is a decision that should be transparent in law acts (e.g. retiring toxic products commercial offer, retiring prohibited contents according to the health law –e.g. a blood economic offer). These differences between contents aren't made.

Besides, Spanish act applies to Internet services with an "economic activity".

To see how these rules can operate, we can take a limit case: marihuana contents. You can offer marihuana seeds (a legal commerce activity in Spain), you can discuss about marihuana, practically without limits, but you can't offer marihuana: if you do it, you can be sure that police will identify you and arrest you, and there will be not discussion about the "place" where offer was made or the hypothetical erasing of these contents by police corps). Evidently, police cannot intervenes your personal communications or intervene your public contents without a judge permission.

2.3.2. Legal gaps on ISS law

ISS law and its application have some dark zones, as it will be shown on next parts of this work, but there are important law gaps and it's important to remark that situation.

In Spain's case, ISS law doesn't differentiate between professional services and private use of net and it is not clear (transparent) on defining the limits of the application or the activities concerned. Sections 1 and 2 of ISS Act have no reference to the activity concerned. The motivation of the Act fixed a wide

concept of ISS,[9] which represents an 'economic activity' (but it is not explained: main economic activity, any commercial activity, only money transfers, even without profit, non-profit organisation that do some economic activity to self-sustain?).

Another legal gap refers to the legal interest protected, because section 8 of ISS Act establishes some conditions as to when the restrictions can apply: public protection for minors or minorities, criminal offences, public health, public security, minor's protection, consumer's protection. That's a list directly copied from the directive. So, it is not adapted to legislative instruments as minor's protection law, criminal law...

Generally the law regarding these matters establishes restrictive administrative acts and it is normal to think that these administrative powers are concerned. But some legal constraints aren't respected: 1) legal description (faults and reasons for actions should be previously fixed), 2) special procedure of legislative bodies, 3) judge's permission in fundamental freedom cases. ISS Act has not made any reflexion about it, and it is applied on a few cases, as I'll show you briefly.

In this matter we have to recognize that administrative sanction powers can be not effective at all, as warn us Professor A. Nieto at *Derecho Administrativo Sancionador*, 2nd ed., and accept that Spanish constitutional doctrine is clear: no aprioristic legal restriction can be fixed on fundamental rights matters.[10] And finally, Decency Communications Act case argument was clear: some protections can be disproportional to the hypothetical profit that they can wait to obtain (Custos, 1997; Boix Palop, 2007a).

In the economic area, some problems are misunderstanding. The majority of Net contents are the result of economic processes. Big communication enterprises let the users a space and that simple operation is possible by advertising or direct payment by user. So, there can appear economic behaviour that can create market distortions. In our days too many economic problems can rise. At macro level, code problems (as Microsoft case shows) or no neutral regulations (see FCC neutrality principle interpretation and Net 'fathers' opinion) can provoke economic disrupters (e.g. servers filtering technologies, a solution taken to promote web traffic as a result of web 2.0's macro-architecture).

At the horizontal level, some bloggers are financed by hardware or software producers. In a strictly legal consideration, the concept of 'neutral information' is affected. Judges accepted –in the US– to apply the journalist protections to a blogger and that's a radical change, because an opinion is protected as an objective information, so where is the line between these concepts? Is economic interest, expertise, objectiveness itself?

9. Even internet journals are concerned, so, will press companies have 2 different regulations: Press Act to journalistic function (for contents) and ISS Act for electronic forms? Even public services are included by authors and administrations in a ISS Act.

10. See STC 171/1990, STC 172/1990.

In the Spanish case, the mixing of professional and non-professional sectors is a dark zone; in the next paragraphs we will see what kind of problems can be created by that legal gap.

3. Judicial cases referring dissemination of information

In this section I'll point out some of the most relevant and recent judicial cases referring dissemination of information. Some of them are simply cases of freedom of expression, in other cases the judicial decision turns over the ISS Act.

SGAE vs. Asociación de Internautas, SGAE vs. Frikipedia

The Asociación de Internautas (Internet users association, AI) was persecuted by the SGAE (authors and editors society) for honour offences. AI published on his website a critical text about the SGAE activities (to collect the intellectual rights compensation for public communication); the text criticized the methods for the collecting activity including the words "mafia" and "ladrones" (thieves). The judge condemned AI to pay a 36.000 indemnity to SGAE on honour offences.

The "frikipedia" administrators (humoristic wikipedia) were persecuted on the same arguments because a Google bombing (searching "ladrones" the first result was the SGAE website): the indemnity was 600 € (this case is a steady –closed– case).

Putasgae.org

The Asociación de Internautas was prosecuted by SGAE on the suspicion that AI was the author of the website putasgae.org. Another time the honour offences were the main argument. The website contents were similar to the contents persecuted in the first case (SGAE vs. Asociación de Internautas), which were re-linked on the AI website. This case is waiting for the EU Justice Courts prejudicial judgement on 2001/31/EC Directive (which excludes liability for external contents –as the ISS Spanish act reproduces).

Note: On national domain names (.es), the legal framework establishes an administrative function for a commercial public service who exercises some administrative powers (see Malaret & Alonso, 2007).[11]

11. The ICANN delegation of first level domain names (country domain names) in Spain is for Red.es, a commercial public service under the authority of Industry, Tourism and Commerce Minister. The legal framework for the execution of policies on this subject is mainly on government hands. Actually, no formal act establishes the regime, the procedures or the material norms for the exercise of administrative powers (only a reference in the 2000 complementary to the budget act, and a minimal legal authorization for Red.es on the assignment functions):

El jueves

"El Jueves" is a popular satiric magazine. The cover for the edition of July, the 3rd of 2006 week edition depicted the Spanish prince and princess in a sexual scene (the prince saying to the princess –oh, if you are pregnant, this is the closest to work I have been! –the joke was a criticism to a government aid for new parents). The National Audience "kidnapped" (provisionally and later confirmed) the magazine, so the judge ordered to take them away from commerce, because an hypothetical honour offence, and prosecuted the directors of the magazine on a penal fault procedure (injuries to the crown). The whole society (people, journalists, academics) were radically opposed to the judicial action of kidnapping: the censured image was replicated everywhere on the net (on blaze-like ways) and during the next weeks it was the reason for a popular wave of protests (including collective burnings of kings pictures) which were prosecuted on the same legal reasons of the Jueves case. The results of the judicial case was 'guilty' and El jueves had to pay a 3.000 € fine (and similar fines to some kings pictures burners).

Ramoncín vs. Alasbarricadas

Alasbarricadas is a web-forum of the anarchist syndicate CNT ("a las barricadas" is the title and the first words of the anarchist hymn); the access to the forum is free and open (not only the syndicate members). One of the participants called "gilipollas" to a SGAE director council member, known as Ramoncín, others blame him and other participants "menace" him ("if I meet Ramoncin on the street..."). Ramoncin was a subversive author on the 70's and 80's and actually he's a director of SGAE [professional association to protect intellectual property rights].

Ramoncín had been trying to contact the organisation of alasbarricadas.org, demanding on to erase those contents, as an honour offence. The adminis-

---

18th "Additional Disposition" wich establishes the authority to establish a procedure for the assignement of domain names on .es level (as a commercial public service, and in "generaly adopted practices" ways); that legal authorization was completed by the 6th Additional Section of the 34/2002 Act (transposition of 2000/31/EC Act).

These legal norms authorized Red.es to reserve or withdraw some domain names: 1) Red.es can reserve whole domain names or some parts of them that, as related on RFC, can confuse users ("wai", "http", technological denominations), 2) Red.es can reserve official denominations as names of cities, constitutional bodies, etc..., 3) Red.es can withdraw illegal domain names on general terms or intellectual or industrial property terms, which can be retired on the basis of a judicial mandatory. The ISS Act doesn't configure the activity as an administrative activity, but as a commercial activity; the only reference to administrative concepts are references to the principles of administrative law –procedure, hearing– for some administrative powers that can be exercised by Red.es (ISS act and other legal instruments don't clarify what are the space for these administrative powers, and we think that reserve of domain names or lists of prohibited domain names are, and Administrative Law should be applied –and administrative judges should act, but reglamentary acts let these matters to private procedures).

trators didn't erase the contents, so Ramoncin went to court, who ordered the erasing of the contents to the webmasters (the judicial mandatory was quickly obeyed). [The main arguments for judicial decision was the application of the ISS Act to this forum and, then, the definition of conditions for effective control or knowledge of contents (in these cases, the ISS is responsible for third person's contents)].[12]

The decision is sustained by the "abnormal identification" of website administrators, in application of legal obligations under ISS Act, and equally by honour offences because it "[was] far from the neutral position supposed to constructive criticism". But which one is the real legal reason?: offences or the ISS law duties? Well, ISS Act says that fundamental rights contents have to be limited by judicial decision, and specifies website kidnapping (section 11.3). So that should be the reason, and not the difficulties of private actors of identifying administrators.[13]

4. Doctrinal dark zones

4.1. Dark zones on ISS application

The 'El jueves' case has shady zones. Probably, the test made by the judge on the provisional measure (kidnapping) was legally unfair because freedom of expression falls on privacy cases but not absolutely on criminal cases, because there we have an absolute right against a "legally protected good", lower protected than another absolute right (as privacy, as well),[14] and the attention shall be focused on the proportionality test. The problem, as the Constitutional Court decisions shown us on several cases is that law can be wrongly applied. The third element of the test (1. adequate, 2. necessary in a democratic system, 3. proportionality *stricto sensu*) can drive the judge to a positive action, as a parliamentary body does (González, 2004). In that case, the legal problem is that the other elements (adequate, necessary) are usually underweighted.

True, in this case, the government admitted that the image was replicated on the Net, and this fact forces us to question that legal instrument (see Alonso, 2007). Maybe, kidnapping was not "adequate" or "necessary" in a democratic

12. The economic activity is not indicated at the judicial decision but there's a rumour around that (...PayPal was responsible for the "economic activity" of administrators).

13. Judge's decision say that ISS duties included collaboration with authorities (Argument #5.3 in fine) and "even the assumption of ofensive nature contents and its difusion even by passive actitude" (colaborando e incluso asumiendo la difusión de un contenido difamatorio y su prolongación en el tiempo, por su actuación omisiva). That's true, but only in the case of private claims; the judge's order to erase contents was quickly obeyed. Here is clear the melting of ISS law and fundamental rights content, even if it isn't allowed in the ISS Act.

14. Some criminal law considerations can be made, because the injury crime is a behaviour crime and the publication was already the criminal fact –so the crime is not committed in every sale.

state, and proportionality *stricto sensu* can be questioned. Flame replication of the kidnapped picture is proof of how censorship is useless in the Internet age. Furthermore, the whole society disagreed, included the whole sector of journalists, with this decision, which was another evidence of its disproportional character. That's the position of the 'driver on the wrong side of the road' (Van Klink & Prins, 2002 –authors advise the public powers to act as 'roadmender').

The majority of judicial cases are based on the SGAE activities and the criticism from the civil society. These are cases to discuss about the freedom of information and expression and their limits, and constitutional doctrine on this.

But the arguments are based always on irrelevant questions, legally speaking, like calling (anonymously) the chairman of a private association a thief from a public forum, or insult a singer which used to spit on their public during concerts. All this petty claims create confusion about administrators or third person contents (in all of this ISS Act it has been confusingly applied to non-profit activities). Thus webmasters liability for third person contents is a mistaken application of law. Two new dangers are coming: private censorship and self-censorship.

The main problem on such cases is that accepting the Administrators liability is to strength private power positions. So, if Administrators have to obey private corporations, private censorship will arise; in some cases it has happened already (e.g. CB Services, a financial intermediary put pressure onto a blogger, who finally accepted to change some parts of an opinion article about the CB Services business practices). Therefore, the guardians of free expression will not be judges anymore, but private organisations.

Concerning self-censorship, journalists and individuals self-imposed silence has always been something to be worried about (see Boix Palop, 2007b), because it is equally dangerous as public or private censorship in a democratic society.

I think that limits of expression are no clear, and some reflexion will be necessary to find the points of balance. Principle of proportionality is a good system, but can carry the judges to a personal opinion. So, when we do the proportionality test, we have to consider not only if the actions are adequate or necessary for a democratic society, but also if they are socially accepted behaviours (adequate or necessary ones) and thus capable of extending and getting richer democratic processes and debates or, on the other hand, if those expressions stop or difficult public debate and democratic process.

4.2. Judicial policy and democratic society

But, what are the future consequences of such judicial decisions, on legal and social understanding?

These ineffective limitations only can confirm the gap between constitutional bodies and society which it is a problem of legitimacy because authori-

ties are seen as an aristocratic class (Muñoz Machado, 2004); in addition, some of these limitations can be clearly unconstitutional (Boix Palop, 2002, referring to wide administrative powers over freedom of expressions contents).

Those judicial decisions are ineffective because the new horizontal structure of Net need. This situation demands some thinking, as it "imposes the acceptation of its intrinsic complexity" (Sánchez 2005).

Outside, the street has a reactive attitude to this kind of judicial decisions (Ramoncín was spontaneously attacked during a music festival, king's pictures were burned). In our case, these disputed judicial decisions did not have the effect they were looking for. This shows that there was a popular opposition that wanted to express those dissident points of view (e.g., a political incorrect language). But the question is wrongly formulated: the Internet is not a vertical sector of activity and the common behaviour is much more similar to art (freer than other types of communications) or public conversations, public debates and public expressions (even the speaker-on-the-corner ones), as I proposed before (Alonso, 2008; see, for Spanish judicial cases analysis about this question and other relevant Internet characteristics as anonymous communications, Roig, 2007). Or, in the words of the comedian Lenny Bruce: I'm guilty because I repeat popular expressions of quotidian life (referring to blow-job).

To confirm those judicial decisions will not only be a danger for freedom of information and expression, but will also provoke a growing uniformity and other dysfunctions. In accordance with Sunstein's arguments "nations are far more likely to prosper if they allow their citizens the right to think the unthinkable, discuss the unmentionable, and dare to challenge the unchallengeable" (Sunstein, 2008).

Consequently, legal doctrine has important contradictions. On the one hand we have a strict judicial policy to some dissident expressions that were inoffensive (at least until the judicial decisions) in a questionable application of ISS Act (because there were no business and in some cases the activity was an humoristic or political activity). On the other hand some hate expressions (denial of holocaust) were (surprisingly) legalized (decriminalized) by Constitutional Court.[15]

That situation reminds us the solution of 'Yahoo!' Nazi website case. In France, these type of expressions are prohibited, but in the US they are perfectly legal expressions (the server was located on US territory). Finally, society (internet users mainly) rejected those expressions and Yahoo! decided to erase those contents, in line with the 'market forces', or user protests. By doing so, in Spain some hate expressions like the apology of Nazism can be presented as a 'historical content' that justifies the murder and prosecution of minorities while some dissident expressions are meticulously analyzed (under the basis of professional law as ISS Act).

15. STC 235/2007, 7 november 2007.

5. Conclusions

Some authors discussed about the future of broadcasting and ISS law. A few of them believed that with the arrival of the Internet the new broadcasting law was going to be softer than actual laws (Boix Palop, 2007a, Gómez Carnota, 2004), while others believed in the opposite evolution, that ISS were going to be under the broadcasting law (Tornos, 2002). Things were going to be more complicated than that.

As I have shown, the treatment of Internet contents is legally unfair and not clear, because the non-economic activities are under the ISS law on a weird way. So, legal framework is deficient, confusing and an open highway to arbitrariness.

In Spain legal practice and legal debates are less clear about these questions than in other countries (like in the USA). Legitimacy problems of constitutional bodies and the Administration itself (Sanction powers included, see Nieto, 2004) take the legal operations to a dark zone. This is the zone where the economic activity and non-professional services collide, but authors that warn us about this legal gap don't analyze the kind of legal space these cases belong to, commercial law or constitutional law. Both Sunstein (2003) in the USA and Villaverde (2007) in Spain, identify this problem but no solution is given.

I've tried to make a definition of this problem (professional vs. non-professional communications), distinguishing the main activity: commercial purposes against other types of main activities (i.e. political expressions, art and humour expressions, public services), this is the way it is considered on broadcasting law (it only applies to commercial activities/services).

Later I have identified an economic law space for activities that have economic consequences. It is important to analyze the economic problems related to code matters. It is also important to think about the individual's information/opinion that can modify market conditions.

New economic behaviours can arise. Are we prepared to analyze or even judge an economical offer made by an Internet provider to users? E.g. "Get money or a gift subscribing and using an XXXX –name of advertiser– account").

In conclusion, we have seen that legal framework evolving dissemination of information is confusing. In consequence, judicial decisions move on arbitrariness spaces (opened by deficient ISS Act definitions) and treat political or humoristic expressions with a professional legal framework. That's a problem for the public and legal debate about freedom of expression and political debate. I proposed that legal framework for ISS must define clearly the definition of ISS, as the broadcasting law does. Why? Simply because the new technologies are more horizontal and to think on vertical structures is useless: that situation will provoke the revolts of common sense on a legal and societal view.

References

1. Boas, T.C. (2006) "Weaving the authoritarian web. The control of Internet use in nondemocratic regimes", in Zysman, J.; Newman, A. (Eds.). *How revolutionary was the digital revolution? National responses, market transitions, and global technology*. Stanford: Stanford University Press, 2006, pp. 370-371.
2. Boix Palop, Andrés (2007a). "De McDonald's a Google: la ley ante la tercera revolución productiva. Revista *Teorder*. 2007, nº 1.
3. Boix Palop, Andrés (2007b). "La traslación de pautas de control público al nuevo audiovisual de proximidad. *Revista General de Derecho Administrativo*, nº 14, febrero 2007.
4. Custos, Dominique. "Liberté d'expression des adultes et protection des mineurs sur le réseau Internet selon la Cour suprême des États-Unis". *Revue du droit public et de la science politique en France et à l'exterieur*, T. XCIII, nº 6 (1997).
5. Fernández Farreres, Germán. *El paisaje televisivo en España. Características e insuficiencias del ordenamiento de la televisión*. Pamplona: Aranzadi. 1997
6. Van Klink, B.M.J, Prins, J.E.J. *Law and Regulation for the information age*. Amsterdam: IOS Press. 2002.
7. Malaret, Elisenda; Alonso, Carles. "Els serveis públics informacionals: l'emergència de nous serveis públics en la societat de la información i el coneixement". *Revista Catalana de Dret Públic*, nº 35/2007.
8. Muñoz Machado, S. "La libertad y el poder en la gran telaraña mundial", en Gómez-Reino y Carnota, E. (Coord.). *Telecomunicaciones, infraestructuras y libre competencia*. Valencia: Tirant lo Blanch. 2004, p. 67.
9. Nieto, Alejandro. *Derecho administrativo sancionador*, 2nd ed. Barcelona: Ariel. 2004.
10. Sánchez, Jordi. *La democràcia electrònica*. Barcelona: Edicions UOC. 2005, pp. 26-27.
11. Lessig, Lawrence. *El código y otras leyes del cyberespacio*. Buenos Aires: Taurus. 2002.

    — *Code: version 2.0*. New York: Basic Books. 2006.

    — *Free Culture*. New York: The Penguin Press. 2004.
12. Roig, Antoni. "Dret public i tecnologies de la informació i la comunicació". *Revista Catalana de Dret Públic*, nº 35/2007, pp. 343-344.
13. Sunstein, Cass R. *Republica.com. Internet, democracia y libertad*. Buenos Aires: Paidós. 2003.

    — *Why societies need dissident*?

Privacy and free speech in social networks

Luis Fernando Rodríguez García
Ph.D. Researcher, UNED

Abstract. In spite of the cyber-libertarian view on the Internet being defeated by the paternalist school, the underlying arguments of the cyber-libertarians remain. The internet is changing the relief of some human rights, since interactions are being held in new environments far from traditional socialization structures. In particular we shall examine how privacy and freedom of speech are affected and re-shaped by the new phenomenon of social networking. Moreover, traditional rights of privacy and communication privacy are to be revisited and widened to face the new threats the cyberspace represents.

Keywords: Privacy, freedom of speech, social networks

1. Introduction. The backdrop debate

In a famous statement, Eric E. Schmidt, the current CEO of Google Inc said that "the internet is the first thing that humanity has built that humanity doesn't understand"[1].

Shortly before, in his famous *A Declaration of the Independence of Cyberspace*[2] made at Davos, Switzerland, and published *online* on February 8 1996, the cyber-libertarian John Perry Barlow informed the "Governments of the Industrial World, you weary giants of flesh and steel" that "You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear... Cyberspace does not lie within your borders" And then he remarked: "Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion". This powerful challenge to traditional regulators reflected the cyber-libertarian spirit that law and norms could not succeed in cyberspace due to the physical nature of the place: "Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here". Moreover, this ethos was

1. Speech, The Netscape Communications Developers' Conference, October 18 1996.

2. "A Declaration of the Independence of Cyberspace" was an influential early paper on the applicability (or lack thereof) of government on the rapidly-growing internet. It was written by John Perry Barlow, a founder of the Electronic Frontier Foundation, primarily in response to the passing into law of the Telecommunications Act of 1996 in the United States. The Declaration sets out, in sixteen short paragraphs, a rebuttal to government of the Internet by any outside force, specifically the United States.

founded upon the twin foundations of "unregulability of bits"[3] and the ability of internet users to transcend borders without challenge[4]. The internet was shown as a no-go place for the law.

Barlow and other cyber-libertarians suggested there were no functional mechanisms for pushing deviant behavior back towards the standard that could be used to enforce traditional laws in cyberspace, as is used in the traditional legal-regulatory control system such as imprisonment or fines would prove to be ineffective against digital entities that have no physical identity or fiscal funds. Thus traditional laws and law-making, based upon the concept physicality, were rendered ineffective in cyberspace in the very sense of the word. In addition, the lack of borders within cyberspace suggested to cyber-libertarians that traditional state sovereignty, based upon notions of physical borders, would be undermined in cyberspace as individuals could move seamlessly between zones governed by differing regulatory regimes. This, the cyber-libertarian believed, would foster regulatory arbitrage and undermine traditional hierarchically structured systems of control. Basing their beliefs upon these two foundational concepts the cyber-libertarians argued that the lack of a physical presence to cyberspace effectively undermined traditional laws and law-making, which are based upon the concept of physicality of goods and persons. As Barlow claimed, "your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here".

The cyber-libertarian thesis was quickly answered back by the cyber-paternalists, who demonstrated that in fact the lack of effectiveness of traditional legal-regulatory control systems did not mean lack of regulation. On the contrary, it facilitated the substitution of alternative private regulatory systems[5]. John Reidenberg demonstrated how these systems could, through the application of design controls, act as proxies for courts and law-enforcement authorities[6]. This concept of control through technology went on to be developed and applied by a number of eminent cyberlawyers, including Mark Stefik[7], Mark Lemley[8] or Cass Sunstein[9]. It was called *Lex Informatica.*

---

3. The unregulability of bits thesis was based on the hypothesis that computer data as mere flows of digital information, which had no physically or mass, could not be effected by traditional models of regulation which are based upon physically.
4. Johnson D and Post D, "Law and borders .The Rise of Law in Cyberspace", 1996 48 Stan LR 1367.
5. Joel Reidenberg demonstrated this thesis by indentifying two types of systems: 1. Regimes based upon contractual agreements such as those between ISPs and customers and 2. Regimes built upon the network architecture such as the technical standards promulgated by bodies like the Internet Engineering Task Force (IETF).
6. Reidenberg, J, "Governing Networks and Rule-Making in Cyberspace, 1996, 45 Emory Law Journal 911; "Lex Informatica: The Formation of Information Policy Rules Through Technology", 1998, 76.
7. Stefik, M, The Internet Edge, 1999, Cambridge, MA: MIT Press.
8. Lemley, M, Place and Cyberspace, 2003, 91, California Law Review 521.
9. Sunstein, C, Republic.com, 2001, Princeton, NJ: Princeton UP.

Eventually, the cyber-paternalist school of thought has become the dominant school of cyber-regulatory theory over the last ten years. Although the cyber-libertarians lost the debate, the underlying arguments of the cyber-libertarians remain: it is extremely difficult and costly to enforce traditional legal-regulatory control systems within cyberspace, due to a variety of factors including a relative degree of anonymity, lack of physicality, digitization of content, environmental plasticity and the international or cross-border nature of the network. Finally, they succeeded in demonstrating the problems law-makers would have to face and are now facing in applying traditional legal-regulatory systems in the network environment. This is happening even when fundamental rights are involved[10]. In fact, the internet is changing the relief of some human rights, since interactions are being held in new environments far from traditional socialization structures. In particular we shall next examine how privacy and freedom of speech are affected and re-shaped by the new phenomenon of social networking. These social technologies are altering the architecture of public life and they will go further in a way which deserves some concrete advice about how to cope with them.

2. What are social networks?

Around the world, an increasing number of people are joining social network sites like MySpace, Facebook or, in the case of Spain, Tuenti. Once logged in these systems, participants are asked to create a profile to represent them digitally. Using text, images, video, audio, links, quizzes and APIs, users generate a profile that expresses how they see themselves. These profiles are put together into a large web through 'friends' or 'contacts' lists. Participants can mark other users as 'friends'. If that other person agrees with the relationship assertion, a photo of each is displayed on the profile of the other and both can then access the profiles of each other. Through selection, participants develop a 'friends' list.

The collection of 'Friends' is not simply a list of close ties (or what we would normally call 'friends'). It can include weak ties in everyday life. Anyway, this feature allows participants to articulate to their audience –or who they see as being a part of their world– within the site. While social networks have millions of users, most participants only care about a handful of them, which is typically represented by the list of Friends. If an individual imagines his profile to be primarily of concern to a handful of *close* friends, he is quite likely to have very few 'friends' and he will keep his profile private. If he wants to be speaking to more people, his contacts list is likely to have hundreds of Friends who are roughly of the same age, have the same interests, listen to the same music and so on. He can also prefer to keep his profile publically visible and

10. Let us remember Barlow, "Your legal concepts of property, expression, identity, movement, and context do not apply to us".

accessible to any user. If the profiles´ social network is indexed by a search engine, they will be accessible and easy to find for anyone.

Profiles and contacts lists are two key features on social network sites. The third one is a public commenting feature ('comments on the Wall). This feature allows individuals to comment on their friends' profiles. These comments are displayed prominently and visibly for anyone who has access to that profile.

These three features –profiles, contacts lists and comments– comprise the primary structure of all social network sites. Although these sites allow visitors to wander through lists of users –with profile pictures– and communicate with anyone who has a visible profile, the primary use pattern is driven by pre-existing friend groups in offline life. People join the sites with their friends and use the different tools to hang out, share cultural artifacts and ideas and communicate with one another.

3. Social networks: private, public or what?

3.1. Internet structure: beyond the classical free speech

At a first step, cyberspace is challenging to interpretation. Doctors say that to make the right diagnosis is 70 per cent of the remedy. Therefore, a good deal of the internet legal problems can be properly resolved if we are able to diagnose –from ancien greek, διάγνωσις, knowledge–, that is, if we understand what the internet is really is.

It is my view the internet must be considered before and after all things a prolongation of public space, before a mean of communication or anything else. As any other public space –like streets, squares, leisure centers or gardens– the internet displays itself like an environment where people can gather publicly through mediating technology. In some senses, this mediated public place is similar to the unmediated publics with which most people were familiar until now.

Regarding freedom of speech, the internet has extended its exercise wider than ever could be imagined. As long as he has got an internet connection, anyone anywhere around the world can publish and get information –pictures, videos, text or sound– indiscriminately.

3.2. Social networks in the world wide web

Unlike the World Wide Web, social network sites are not to be considered as another modality of public space upon the public space of the internet. Most social network profiles are private and this makes a difference. Every participant decides if his profile is open or limited to some people in particular. Thus, private profiles compose a net of tangent circles as wide as the social network is.

In the end, social networks are a prolongation of the relationship which the user keeps with his circle of relatives, friends and acquaintances –weak and strong ties– in *offline* life. Activities that in the past required a meeting around a table and having a coffee in order to show holiday photos; or a phone call, as to congratulate a birthday, can be done via social networking and be shared with as many people as are connected. In this very sense, networks have become a prolongation of everyday life activities.

Perhaps it is important to highlight that social networks are in no way unrelated to the rest of World Wide Web. Information published in profiles presents four properties, three of which are shared with the internet environment. The forth one is typical of private profiles on social networks, because of what we could call their "defined" audience. These features are the following:

3.2.1. Persistence

What you say sticks around. This is great for asynchronous communication, but it also means that what you said at 15 will still be accessible when you are 30 and you will have purportedly outgrown those childish days.

3.2.2 Possibility of being searched

Everything you do on the Net produces data. Most of this information can be found thanks to the increasingly mighty search engine. The content of the ordinary chatter of friends which is exchanged through social networks is saved in a searchable form.

3.2.3. Replication

Digital bits can be copied; this means that you can copy an image from one place and paste it onto another place. It also means that it's difficult to determine if the content was doctored. On the other hand, once the content is uploaded, monitoring becomes an impossible task.

3.2.4. Defined audiences

On the internet, persistence, the possibility of being searched, and replication introduce audiences that were never present at the time when the expression was created. On the contrary, closed profiles allow us to define who will be our audience. Unlike journalists, participants in social network sites need not to imagine their audience; it has been selected by them and, therefore, they know it.

One way or another, these properties are changing all of the rules of communication as it has been known until know. You cannot even begin to com-

pare the traditional mass media –its conduct, its aims, its financial support, etc.– to this new mean of communication.

4. Widening privacy right

4.1. Widening communication privacy

One of the most peculiar aspects of the internet is its two-faced form. The internet may be considered as a mass media. In fact, any user can go further than any newspaper or television channel has ever reached. All these publication aspects are no doubt protected by freedom of speech.

At the same time, the internet also offers a traditional mean of communication like mail or telephone. Beyond any shadow of doubt, both have been traditionally protected on the ground of communication privacy. Nevertheless, similar services, in a digital way, are being offered via the internet, like electronic mail, instant messaging in social networks or software applications like Skype, which allows users to make voice calls over the Internet thanks to a proprietary Internet telephone (VoIP) network.

Old mail or phone communications are characterized by being a bilateral channel. A private letter could only come to one mailbox, the call to a friend could only involve one phone. But, on the contrary, new internet devices permit similar communications by multilateral channels, as happens with instant messaging and social networks. This way, birthday congratulations are shared on the wall of a profile. Weekend plans are arranged through profiles in place of numerous phonecalls as in the past. All these communication exchanges remain strictly limited to a few users, selected by the communicants, and that makes them worthy of the right to communication privacy. Moreover, the private character of these communications is assumed by the communicants.

Nevertheless, this new space of communication between individuals has not yet found place in the legal system or rights and liberties in Europe. From the point of view of the right to respect for one's correspondence, the European Court of Human Rights interprets the right to respect for private and family life (Article 8, European Convention on Human Rights) in the sense that it aims to protect the confidentiality of private communications (*B.C. v. Switzerland*, no. 21353/93, Commission decision of 27 February 1995). As such has been interpreted, it covers the following areas:

- Letters (*Silver and Others v. the United Kingdom*, judgment of 25 March 1983, Series A no. 61, p. 32, § 84), including packages seized by customs officials (*X v. the United Kingdom*, no. 7308/75, Commission decision of 12 October 1978, Decisions and Reports (DR); 16, p. 32);
- Telephone conversations (*Klass and Others v. Germany*, judgment of 6 September 1978, Series A no. 28, p. 21, § 41; *Malone v. the United Kingdom*, judgment of 2 August 1984, Series A no. 82, pp. 30-31, § 64;

Margareta and Roger Andersson v. Sweden, judgment of 25 February 1992, Series A no. 226 A, p. 25, § 72) and telephone records (*P.G. and J.H. v. the United Kingdom*, no. 44787/98, § 42, ECHR 2001 IX), even if the aim is to intercept the conversations of a third party (*Kruslin v. France*, judgment of 24 April 1990, Series A no. 176 A, p. 20, § 26);

– Pager messages (*Taylor-Sabori v. the United Kingdom*, no. 47114/99, 22 October 2002);

– Older forms of electronic communication such as telexes (*Christie v. the United Kingdom v. the United Kingdom*, no. 21482/93, Commission decision of 27 June 1994);

E-mails have not yet been included but they could, in the light of the admissibility decision in *Copland v. the United Kingdom* (dec.), no. 62617/00, 7 March 2006.

It is my view that communication privacy rights must cover these multilateral means of communication, as the users can keep the channel closed to others. This thesis relies on the Court´s support, that recognized the confidentiality of private communications in favor of a private mean like a private radio (*X. et Y. v. Belgium*, no. 8962/80, Commission decision of 13 May 1982, Decisions and Reports (DR) 28, p. 112); though not when it is on a public wave band and is thus accessible to others (*B.C. v. Switzerland*, no. 21353/93, Commission decision of 27 February 1995). Such a criterion can be apply upon social networking.

4.2. Widening privacy

On the other hand, the extension of confidentiality to private communications must be framed into the extension of concept of privacy, where its foundation lies.

In this respect, the European Court of Human Rights interprets the right to respect for private and family life (Article 8, European Convention on Human Rights) in the sense of it seeking to protect four areas of personal autonomy: private life, family life, the home and one's correspondence. According to its case law, privacy encompasses the following areas:

– Aspects of an individual's physical and social identity (*Mikulić v. Croatia*, no. 53176/99, § 53, ECHR 2002 II; *Odièvre v. France* [GC], no. 42326/98, § 29, ECHR 2003 III)

– One's picture (*Schüssel v. Austria* (dec.), no. 42409/98, 21 February 2002; *Von Hannover v. Germany*, no. 59320/00, §§ 50-53, ECHR 2004 VI);

– The right to self-determination and personal autonomy (*Pretty v. the United Kingdom*, no. 2346/02, §§ 61 and 67, ECHR 2002 III);

– Surveillance of communications and telephone conversations (see Halford, cited above, § 44; *Weber and Saravia v. Germany* (dec.), no. 54934/00, §§ 76-79, 29 June 2006).

In most of the social network profiles people share some parts of their life with their contacts. This information consists of photos, videos and comments linked more or less with their everyday life. Although it is connected with personal issues, most of this material cannot be considered as intimate, according to the general concept of privacy and intimacy. What we are sustaining here is that information stored and shared in social networks must not be taken out by foreign users without the consent of the user-publisher.

This extension of privacy can be upheld on the ground of the previous European Court of Human Rights doctrine:

1. First, there is no exhaustive or rigid definition of the notion of private life (*Niemietz v. Germany*, judgment of 16 December 1992, Series A no. 251 B, p. 33, § 29) but this is a broad term (*Peck v. the United Kingdom*, no. 44647/98, § 57, ECHR 2003-I; *Pretty v. the United Kingdom*, no. 2346/02, § 61, ECHR 2002 III)
2. Second, article 8 secures for the individual a sphere within which he or she can freely pursue the development and fulfilment of his or her personality (see *Brüggeman and Scheuten v. Germany*, no. 6959/75, Commission's report of 12 July 1977, Decisions and Reports (DR) 10, p. 115, § 55), it is not confined to measures that affect a person in their home or private premises: there is a zone of interaction with others, even in a public context, which may fall within the scope of private life (*P.G. and J.H. v. the United Kingdom*, no. 44787/98, §§ 56-57, ECHR 2001 IX). These considerations can be applied to social networking sites.
3. Although the notion of family life is an autonomous concept (*Marckx v. Belgium*, judgment of 13 June 1979, Series A no. 31, p. 11, § 31, Commission's report of 10 December 1977, Series B-29, p.44, § 69) that cannot involved social networks sites[11]. Anyway, it must be considered that close relationships short of "family life" generally fall within the scope of "private life" (*Znamenskaya v. Russia*, no. 77785/01, § 27, 2 June 2005 and references therein).

5. Conclusions

11. Consequently, the question of the existence or non-existence of 'family life' is essentially a question of fact depending upon the real existence in practice of close personal ties (K. v. the United Kingdom, no. 11468/85, Commission decision of 15 October 1986, Decisions and Reports (DR) 50, p. 199, 207).

People communicate with each other in social networks and show some aspects of daily life that do not fit into the usual concept of privacy. Until now, most of these activities have been taking place in public or semi-public, and no register is left. In addition, users perceived social network profiles as a personal area, whose access is limited to whom the very user decides. The fact that social network profiles are multidirectional communication channels should not be a qualm here.

The extension of the privacy right can be like the counterweight to the powerful intrusive capacity displayed by the internet, perhaps the most serious threat that has existed so far. It is equitable to expand privacy to those sorts of activities, not intimate but merely personal, which covers the stream of photos, videos and conversations which are shared by social network contacts. Technology has for the first time enabled this exchange, and law ought to have rushing in to help the protection of such a matter of significant public concern. Information stored in social networks must not be taken out by foreign users without the consent of the user-publisher.

From the point of view of the right to communication privacy, there is an obvious need to recognize and protect a new breakpoint which runs between the possibilities of publish *urbe et orbi* in the world wide web and the classical bilateral means of communication. This breakpoint has been put in place thanks to social networking technology. That would explain why the law traditionally has not worried much about this kind of invasion. There was no need for the law to intervene because such an area did not exist. Finally, as long as the emitter may choose his recipients, this exchange must be respected and protected by law.

It is well-known as to how the right to privacy was born in the USA at the end of the 19th century. It is not to be repeated now. In any case, I think it is important to realize that, for Warren and Brandeis, law of defamation, law of literary and artistic property or law of slander and libel and the other remedies known in their age, were not enough to face "recent inventions and business methods [which] call attention to the next step which must be taken for the protection of the person […] Instantaneous photographs and newspaper enterprises have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the house-tops"[12]. Nowadays, the internet has shifted the telegraph, the camera or the high-speed printing press and taken their place in a way that demands new solutions. In a legal sense, we are witnessing the last stage of an old war between free speech and privacy.

Social technologies have altered the architecture of public life and they will go on deeper. It is critical for law-makers to understand how social network spaces are shifting the lives of many people. There are very good reasons

12. Warren and Brandeis (1890), The right to privacy, Harvard Law Review, Vol. IV, December 15, 1890, No. 5.

why they are used, and encouraging them to return to traditional socialisation structures is simply not feasible. Rather than diving deeper into these shifts, I just wanted to offer some concrete advice about how to cope with an emerging re-shaped privacy.

The 20th-century-built walls of privacy show serious cracks now. The parapets are rather useless in facing the threats of the internet. This is the very moment for rebuilding them.

Section Three
ISP accountability and Web 2.0

The problem of liability for illegal content in the web 2.0 and some proposals

Lorenzo Cotino Hueso[1]

Abstract. Liability for illegal contents is a central legal problem of the services offered by the web 2.0. Regulation and case law give no clear answer for the moment. It is indeed a key aspect for the future of most platforms and applications like *Google*, *Youtube, Facebook, Wikipedia*...., and for the web 2.0 itself. In this paper we analyse the main principles of the regulation, and the possibility of using the classical jurisprudence of exemption of liability for illegal content: "the "letters to the editor" doctrine", "the neutral article", and also the diligent attitude of the Internet Services Provider (ISP) that hosts the content. Finally, we indicate some future trends, on the basis of the freedom of speech. We argue that intermediaries shouldn't have accountability and that we should protect the anonym participation in the web. On the other hand, we also indicate concrete key aspects for each case, with the central idea that we have to adapt the solution to the concrete characteristics of each service and case in the net.

Keywords: internet, e-law, liability for illegal contents, intermediaries and service providers, web 2.0, freedom of speech.

1. Introducing the problem and its importance

1.1. The problem

Liability for illegal content in the web[2] is a major issue for the net itself. Furthermore, the problem is the accountability of the ISPs that offer services like connection, content (text, audio, video, photos, programs, etc.) to users of the service. The answer to this problem can change the business model of *Google*, *Youtube, Facebook, Wikipedia*, etc., and can even condition the model of evolution of the web[3]. Nowadays Internet is growing by no less than one third

1. cotino@uv.es, www.cotino.es Professor of Constitutional Law at the Valence University, and coordinator of the web of specialists in Law and Technology, www.derechotics.com. This study is in the frame of the funded research project "Freedom of speech In the Context Of Web 2.0 and Social Networks: Redefinition, Guarantees and Limits", Cotino as main researcher. Ministry of Science and Innovation (DER2009-14519-C05-01).e

2. On liability in general, Cavanillas 2005 and 2007; on liability in the US , Peguera (2007).

3. More about web 2.0 in Fumero (2007) and Cerezo (2007).

by "*heavy users*"[4], who participate creating and spreading content[5]. The main difference with the web 1.0 is that now users can include, interact and select content, and no more be a simply consumer, but rather a "*prosumer*" of information, i.e. both consumer and author[6], in continuous dialogue. "Only in Spain we have ten million authors of content[7].

Including illegal content is a legal risk for ISPs. Alonso[8] talks about a sort of mobbing, "*infomobbing*", when we call for liability of the ISP hosting contents from third parties. If ISPs are responsible for the content, only a few will have the capacity of monitoring and filtering all the illegal content. Worse, there will be a chilling effect, and self-censorship will appear. Thus, a lot of noxious speech, even if legal[9], will be out of the line.

1.2. Material and legal dificulties for fixing liability

In Internet, several are the difficulties to determine private, public and criminal liability. Let's begin with the material difficulties:

- National limits don't govern the net.
- The content is usually added anonymously. So, we have to know its IP number –if possible– and even then it might not be enough.
- The collective spreading of the content makes it really difficult to determine the liability.

Furthermore, there is a lack of regulation in the European Union, since the Directive 2000/31/CE of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). In sum, the ISP has no obligation to monitor the content (art. 15 Directive on e-commerce[10]) and has no liability for the illegal content, but has the duty to remove or block the content when authorities inform it of the illegality. In-

4. More about *heavy users in* Previte (2001), Ferran-Ferrer and Pérez-Montoro (2009).

5. See annual Reports, Fundation Telefónica (2008, p. 159). A 29% of Internet users are "heavy users".

6. Bowman and Wills (2005).

7. In Spain, 63% of the population has an Internet connection (38.7% in 2006), about 28 million people, and one third is about 10 million people. February 2009, http://www.internetworldstats.com/stats.htm)

8. Alonso (2008, p. 42).

9. More about the distinction between illegal and noxious in *Communication of the European Commission to the European Parliament, to the Council, to the Economic and Social Committee and to the Regions Committee, on illegal and noxious contents in Internet*, October, 16th of 1996 COM (96) 0487.

10. No general obligation to monitor
    1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

termediary ISPs[11] do not elaborate or select the content[12], and don't have real knowledge of the illegality of the content[13]. Regulation, however, doesn't solve the normal problems.

1.3. The key aspects of the legal problem of liability for the content

On the one hand, we have to settle whether every hosting service in the net (from a blog to *Youtube*) can benefit from the legal exemptions from liability. For this purpose, we have to decide whether this kind of services are those of an "intermediary service provider"[14] (art. 16 LSSICE), and "host data given by the user of the service". The general exemption is also possible, according to article 17 LSSICE, for the services that "link to other content or include directories". Blogs, Wikis, video hosting services, images, commentaries, etc…, don't generally have to monitor contents or remove them until they have "real

2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

11. Most of the time we use ISP, Internet Service Provider, but is not exactly what intermediary providers do, in the sense of the LSSICE, as we'll see further.

12. Section 14 of the LSSICE exempts from responsability net and access services "except those that create the transmission, modify data or select them or the users of the data", i.e. those that don't guarantee the technological neutrality of intermediaries. In addition, hosting providers (art. 16.2) don't benefit from the exemption when the user acts under the authority or monitoring of the provider."

13. Number 42 to 44 of the Directive are clear:
"(42)The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.
(43) A service provider can benefit from the exemptions for "mere conduit" and for "caching" when he is in no way involved with the information transmitted; this requires among other things that he does not modify the information that he transmits; this requirement does not cover manipulations of a technical nature which take place in the course of the transmission as they do not alter the integrity of the information contained in the transmission.
(44) A service provider who deliberately collaborates with one of the recipients of his service in order to undertake illegal acts goes beyond the activities of "mere conduit" or "caching" and as a result cannot benefit from the liability exemptions established for these activities."

14. Definitions of the LSSICE: b) "Intermediary service" service that allows applications of the information society or the access to information.
For instance, some intermediary services are: providing access to Internet, sending data on a telecomunications net, copying temporally web sites required by users, hosting data services, applications or services given by third parties and and offering search engines, data access or links to other web sites.

knowledge of them". This is the doctrine of the "*mindoniense*" case in 2008 and 2009[15].

On the other hand, the exemption from liability requires the neutrality of the hosting service, and ISPs should not have selected or generated the content. Web 2.0 allows third parties to integrate content, and users favour it (commentaries in news, blogs, wikis, photos, videos, etc.). It's also usual to select –in an automatic way or not– content from others –links or using *rss* and *xml*, etc.–. There is no complete technical neutrality but, at the same time, there is no collaboration in illegal acts. Web 2.0 is in a twilight zone, with legal uncertainty, waiting for an eventual future European regulation. And the Spanish and European jurisprudence[16] don't solve the problem, don't mention it or are contradictory. On the contrary, in the US, the country of freedom of speech, neither the regulations nor the jurisprudence[17] are afraid of these difficult issues[18]. First, there are some quite flexible tools that can remove more obvious illegalities for the net with full respect to freedom of speech[19]. On the other hand, in favour of freedom of speech, jurisprudence holds no liability from content inclusion by third parties, even if that option has consequences, while waiting for better legal regulation[20].

2. Some options for exemption of liability from illegal content diffusion

2.1. The constitutional doctrine of letters to editor could illegalize all sna

Newspapers are not responsible for "letters to editor" sections if they have been diligent in identifying the letter's author. If not, "when authorising the publication of the letter without knowing the author, we can then consider that the

15. www.mindoniense.com.

16. Cotino (2007).

17. The jurisprudence has decided interesting cases from 2000 (see www.internetcases.com and www.internetlibrary.com).

18. See, Balkin (2004), Sunstein (2001, 2003) and *Non authored* (2004).

19. See Section 512 of the *Copyright Act*, after changes due to the "*Digital Millennium Copyright Act"* in 1998.

20. Stephen J. Barrett, et al. v. Ilena Rosenthal, S122953, 40 Cal.4th 33 (Cal. Sup. Ct., November 20, 2006), available at: http://www.internetlibrary.com/cases/lib_case447.cfm.
"We conclude that section 230 prohibits 'distributor' liability for Internet publications. We further hold that section 230(c)(1) immunizes individual 'users' of interactive computer services, and that no practical or principled distinction can be drawn between active and passive use. Accordingly, we reverse the Court of Appeal's judgment.
We acknowledge that recognizing broad immunity for defamatory republications on the Internet has some troubling consequences. Until Congress chooses to revise the settled law in this area, however, plaintiffs who contend they were defamed in an Internet posting may only seek recovery from the original source of the statement."

media has accepted the content as its own content"[21]. This jurisprudence tries not to open "the door to immune spaces"[22]. This doctrine could destroy *web* 2.0, because it's very difficult or impossible to identify users participating in web 2.0, and it's also negative for freedom of speech.

Another decision, the "Mafius" case, holds this doctrine to extend criminal liability to blog owner for what is said anonymously, mainly for managing it without monitoring IP numbers.

2.2. The doctrine of "the neutral article"

The jurisprudence of "the neutral article" exempts media from liability when it reproduces, with neutrality, information that comes from third parties. This solution could be used when the site includes external content, links to other sites, or other content is "*embedded"*.

Our jurisprudence has very few decisions on this subject. The exemption was not accepted in the "*putasgae"* case, holding that external contents are like own content[23]. On the contrary, the exemption was accepted in *CCOO vs. El Corte Inglés*[24]*:* the publication of a sentence from Internet on their site. We can also mention a Canadian case, Wayne Crookes[25]. The Court held that a link is like a footnote[26].

---

21. Decision of the Constitucional Court (STC) 3/1997, January 13th, Section 3
22. STC 336/1993, Section 7.º,b.
23. Decision of the Provincial Court of Madrid num. 50/2006 (Section 19), February 6th.
24. Decision of the Supreme Court of Madrid num. 663/2003 (Labour Section), July, 23th.
25. Wayne Crookes and West Coast Title Search Ltd. Vs. Wikimedia Foundation Inc. And Anonymous, Supreme Court Of British Columbia, 2008 BCSC 1424 Date: 2008. Available at: documentostics.com/component/option,com.../task.../gid,1455/
26. [29] A hyperlink is like a footnote or a reference to a website in printed material such as a newsletter. The purpose of a hyperlink is to direct the reader to additional material from a different source. The only difference is the ease with which a hyperlink allows the reader, with a simple click of the mouse, to instantly access the additional material.
    [30] Although a hyperlink provides immediate access to material published on another website, this does not amount to republication of the content on the originating site. This is especially so as a reader may or may not follow the hyperlinks provided.
    [31] I conclude that the reasoning of the Court of Appeal in Carter leads to the same conclusion on the narrower issue before me. Readers of a newsletter, whether in paper form or online, who read of a reference to a third party website, may go to that website. I conclude that that does not make the publisher of the web address a publisher of what readers find when they get there.
    [33] As the Court of Appeal observed in Carter, citing the proposition of the New York cases MacFadden v. Anthony and Kline v. Biben, "reference to an article containing defamatory content without repetition of the comment itself should not be found to be a republication of such defamatory content".
    [34] I do not wish to be misunderstood. It is not my decision that hyperlinking can never make a person liable for the contents of the remote site. For example, if Mr. Newton had written "the truth about Wayne Crookes is found here" and "here" is hyperlinked to the specific defamatory words, this might lead to a different conclusion.

The exemption of the neutral article shouldn't only be limited to ordinary mass media and could be useful for web 2.0. Obviously, the decision has to be taken case by case, without *mala fides* and abuse of law (section 7 of the Civil Code).

2.3. The diligence of ISP and its liability

Sometimes, Courts verify the attitude of the ISP. For instance, the collaboration with the Court is welcome, in the *Weblisten* case[27] and the *"aprendizmason.org"* case[28]. On the contrary, in the *"putasgae"* case, the Court doesn't mention the collaboration of the ISP.

In the "alasbarricadas.org vs. Ramoncín" case[29], the ISP is considered responsible of lack of diligence:

- It has information not updated.
- E-mail contact has not proved to be useful.
- There is no coordinator.

What's alarming in this decision is the lack of legal support for these requirements.

In the "Mindoniense" case, on the contrary, no diligence requirements are mentioned. The Court highlights the *bona fides* of the ISP that has censorship software called "Word Censors".

To summarize, if the Exemption conditions fixed by LSSICE and the Directive do apply, then no added liability for diligence (Section 1902 Civil Code) or for other reasons, should be considered. Obviously, as stated above, the decision has to be taken case by case, without *mala fides* or abuse of law.

3. Proposals

Even if there is a sociological and legal trend to limit the freedom of speech to mass media, this right has to be guarantied in the net[30]. The preferent position of the mass media had its justification in the past. Nowadays, this function is done in Internet and not only by official media. Freedom of speech also protects the anonymity in the net, as Antoni Roig has indicated analysing the US jurisprudence (Roig, 2007). Certainly, anonymity is useful for illegal actions, but

27. Preliminary Decision ("Auto") Trade Court nº 2 of Madrid, November, 3rd, 2004.
28. Decision of the Provincial Court of Madrid, num. 835/2005 (Section 14th), December, 20th.
29. Decision of the District Court num. 44 of Madrid, September, 13th.
30. Decision of the European Court of Justice, december 16th, 2008, preliminary reference C 73/07, nº 58-60.

it also favours freedom and participation in the net[31]. "Anonymity is a shield against the majority tyranny", thus its restrictions have to be limited by strict scrutiny[32]. This jurisprudence has been applied in a case of a forum in Internet[33].

If we want to favour freedom of speech[34], we should not ask for liability from the ISP for third parties' content. Following the US, it's better to have efficient tools to remove clear illegal content from the net. The scrutiny has to be case by case, and context based, paying attention to legal relevant aspects:

- Automatic tool for monitoring content,
- Diligence in the selection of content,
- Average of conflicts due to content,
- Evidence that there is an effective knowledge of the content and real possibilities to monitor it,
- Public knowledge of the content,
- Importance of the web,
- Possibility of answer.

Some of those elements are present in the Spanish jurisprudence. For instance, in the *foro para desahogo* case[35] no one is fund guilty because insults were in a web to show discontent or criticism. In *quejasonline.com* case [36] no liability is established because it is considered an informative media. In other cases, the massive difusion of information against someone using e-mail has been considered not covered by freedom of speech[37].

In the decision of the *carta colgada en internet del colegio de las Ursulinas contra una constructora* case[38], the Court considers relevant that "the person voluntarily goes to the web site, and it could be counteracted by other informa-

31. Wolton, quoted by Fernández, J. J. (2004, p. 192). See also Barrat (2004), Morón (2002).
32. Decision of the US Federal Supreme Court, case McINTYRE v. Ohio Elections Comm'n, 514 U.S. 334 (1995).
33. Case John Doe nº1 v. Cahill WL 2455266 (Delaware, October 5, 2005). http://internetcases.com/library/cases/2005-10-05-cahill_v_doe.html. Doe (anonymous name) published texts on a blog where he criticized a Councilman for his management. The Court applied a strict test to lift the veil of his anonymity and unmask his identity.
34. About freedom of speech and Internet in Spain, Fernández-Esteban (1998 a, 1998 b, 1999), Corredoira (1998), Boix (2002), Boix and López, G. (2006), García-Morales (2006) and some of my books and studies.
35. Preliminary decision ("Auto") of the Provincial Court of Barcelona nº 339/2005 (Section 6), May, 24th, second legal argument.
36. Preliminary decision ("Auto") of the Provincial Court of Madrid nº 36/2006 (Section 2), January, 31st. The texts on *quejason-line.com* referred to the wrongdoings of a construction firm.
37. In this sense, in a case of offenses affecting university lecturers by means of collective e-mail messages, the sentence of the Provincial Court of Granada nº 144/2006 (Section 4), April, 7th, excluded freedom of expression being at stake.
38. Appeal decided by sentence of the Provincial Court of Álava nº 55/2006 (Section 1), April, 11th.

tion elsewhere." It is the same argument held in *John Doe nº 1 v. Cahill*. In the *Plataforma Regional Pro-Identidad Leonesa* case[39], there is a context analyses of e-communication[40]. The context can favour freedom, and adapt communication to new possibilities offered by Internet.

References

1. Alonso, C. (2008), "La información en la Red y el principio de neutralidad tecnológica: la libertad de expresión y la difusión de información administrativa", *Revista Vasca de Administración Pública*, nº 81, págs. 15-61.
2. Balkin, J. M. (2004), "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society" . *New York University Law Review*, Volume 79, april, n. 1, págs. 1-58, págs. 46-47, available at http://ssrn.com/abstract=470842
3. Barrat, J. (2004), "El Anonimato como Parámetro Normativo de la Sociedad de la Información" Journal Informática y Sociedad. Vol. 1 No.2, págs. 30-33, available at http://www.itba.edu.ar/capis/jis/index.htm
4. Boix, A. (2002), "Pluralismo y libertad de expresión en la Red", in *Revista española de Derecho constitucional*, nº 65, pp. 133-180, available on the internet.
5. Boix, A. and López, G. (eds.) (2006) *La autoría en la era digital: industria cultural y medios de comunicación*, Valencia, Tirant Lo Blanch.
6. Bowman, S. and Willis, C. (2005), *We Media. How audiences are shaping the future of news and information,* Thinking Paper of The Media Center, available at http://www.openreader.org/wemedia/JackR/We_Media.htm (3/5/2005).
7. Cavanillas, S. (coord.) (2005), *Deberes y responsabilidades de los servidores de acceso y alojamiento: un análisis multidisciplinar,* Comares, Granada.
8. Cavanillas, S. (coord.) (2007), *Responsabilidad de los proveedores de información en internet,* Comares, Granada.
9. Cerezo, J. M. (dir.) (2007), *La blogosfera hispana: pioneros de la cultura digital,* Fundación Orange, Madrid, available on the internet.

39. The sentence of the Provincial Court of León nº 302/2005 (Section 2), December, 19th, decided an appeal against a sentence of first instance which dismissed an action for rectification. Its object was the rectification of certain historical trials which were included in the web of a foundation.
40. More specifically, it states that the web of a political platform is not directed to a numerous and heterogeneous public (which is true and relevant), and can't be subject to veracity (which is debatable, even if our understanding of the concept must be modulated in order to avoid interrupting the process of free speech in the internet).

10. Corredoira, L. (1998), *Los retos de la información en internet. Las libertades de acceso y difusión*. Seminario Complutense de Telecomunicaciones e Información. Madrid.

11. Cotino, L. (2007), "Nuestros jueces y tribunales ante internet y la libertad de expresión: el estado de la cuestión", Cotino, L. (Coord.) (2007), *Libertad en internet. La red y las libertades de expresión e información,* Tirant lo Blanch, Valencia, págs. 133-234.

12. Cotino, L. (2008), *Nuevas tecnologías, desafíos y posibilidades para la libertad de expresión*, Fundación Giménez Abad, available at: www.fundacionmgimenezabad.es

13. Fernández, J. J. (2004), *Lo público y lo privado en internet. Intimidad y libertad de expresión en la red,* UNAM, Instituto de Investigaciones Jurídicas, Méjico.

14. Fernández-Esteban, M. L. (1998 a), *Nuevas Tecnologías, Internet y Derechos Fundamentales*, McGraw-Hill, Madrid.

15. Fernández-Esteban, M. L. (1998 b), "Limitaciones constitucionales e inconstitucionales a la libertad de expresión en internet", in *Revista Española de Derecho Constitucional*, nº 53, págs. 283-311.

16. Fernández-Esteban, M. L. (1999), "La regulación de la libertad de expresión en Internet en Estados Unidos y en la Unión Europea", in *Revista de Estudios Políticos* nº 103, pp. 149-169.

17. Ferran-Ferrer, N. and Pérez-Montoro, M. (2009), "Gestión de la información personal en usuarios avanzados en TIC", *EPI, El profesional de la información*, Julio-agosto, vol. 18, núm. 4, págs. 365-373, available on the Internet.

18. Fumero, A. *et al.* (2007), *Web 2.0*, Fundación Orange, Madrid, available on the internet.

19. Fundación Telefónica (2008), *La Sociedad de la Información en España. Informe 2008*, Ariel, Barcelona, available at: http://e-libros.fundacion.telefonica.com

20. García-Morales, M. J., "Nuevas tecnologías y libertad de expresión: regulación, autorregulación y filtros en internet", in COTINO, L. (Coord.) (2006), *Libertades, democracia y gobierno electrónicos*, Comares, Granada, pp. 33-58.

21. Morón, E. (2002), *Internet y Derecho penal: Hacking y otras Conductas Ilícitas en la Red*, Aranzadi-Thomson, (2ª ed.), Pamplona

22. Peguera, M. (2007), *La exclusión de responsabilidad de los intermediarios en Internet*, Comares, Granada.

23. Previte, J. and others (2001), "Profiling Internet Users' Participation in Social Change Agendas: An Application of Q-Methodology", Faculty of Bu-

siness, Queensland University of Technology, available at: http://arxiv.org/abs/cs/0109058.

24. *Revista Catalana de Derecho Público*, about "La incidencia de las TIC en el Derecho público", núm. 35, 2007.
25. Roig, A. (2007), "El anonimato y los límites a la libertad en internet", in Cotino, L. (Coord.) (2007), *Libertad en internet. La red y las libertades de expresión e información,* Tirant lo Blanch, Valencia, pp. 321-354.
26. Sunstein, C. R. (2001), *Republic.com*, Princeton University Press. (in spanish: (2003), *República.com. Internet, democracia y libertad*, Paidós, Madrid.
27. *Non authored* (2004) "Weblogs in Journalism: Blogging and the Law", available at: http://www.unc.edu/~briman/J221/bloglaw.html (4.3.2005).

Service Providers Accountability

Sergi Torralba
Albert Meroño
Antoni Roig
Institute of Law and Technology, Autonomous University of Barcelona
(IDT – UAB)

Abstract. The goal of this paper is to guide through some obscure parts of the regulation and legislation related to technology. Even if we are not experts on security Internet, we will try to explain the difficulties that lawyers should be aware of when regulating rights and limits in the net. Some real cases related to service providers (ISP and others) are described and complemented with the technological context of each case.

Keywords: Regulation, Technology, Internet, Legislation, ISP.

1. Introduction (end-wire users are transparent to ISP)

Recently there is a trend to make Internet Service Providers (ISP) responsible for any infraction committed by their users. There are technological arguments to hold that may be this is not the correct way.

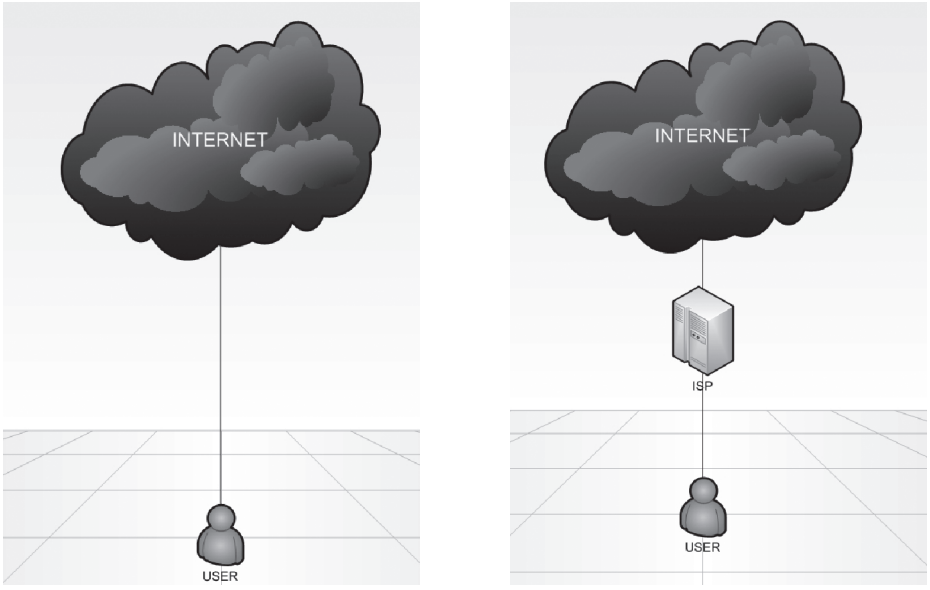
In this introduction, we are going to explain a general framework on how technology and Internet connections have evolved in the last 15 years. In Spain all began with InfoVia[1] in 1995 and its speed was 28.800 bps. Meanwhile, Intel presented the Pentium 133 which has a speed of 133 MHz. Nowadays we have multiple of options to connect to Internet from de evolution of InfoVia, which are the ADSL connections at a speed around the 20 Mbps more than 700 times faster. And the technology has also improved. Some processors like Core 2 Quad Q9650 of Intel have a speed of 3 GHz, and even if it is only 30 times faster, we have to consider that 15 years ago there was only 1core. Now we can have 4, which is similar to having 4 processors working together. Furthermore, in the 90s very few could imagine how many devices would be able to connect to Internet. Not only are computers connected to the Internet, but even some fridges are able to be connected. So, technology went fast, and laws could not follow.

Maybe because at the beginning there was a lack of control and Internet was something only for few people, there has been a misconception with the users. At the beginning of the use of Internet in Spain, users were quite ex-

1. Article about the creation of the creation of InfoVia: http://www.elprofesionaldelainformacion.com/contenidos/1995/noviembre/impacto_de_infova_de_telefnica.html

perts, and Internet was lawless. Perhaps people thought they were connected to Internet directly, and did not realize that there was something between them and the net, may be something like Figure 1.

Figure 1. User vision of the Internet connection



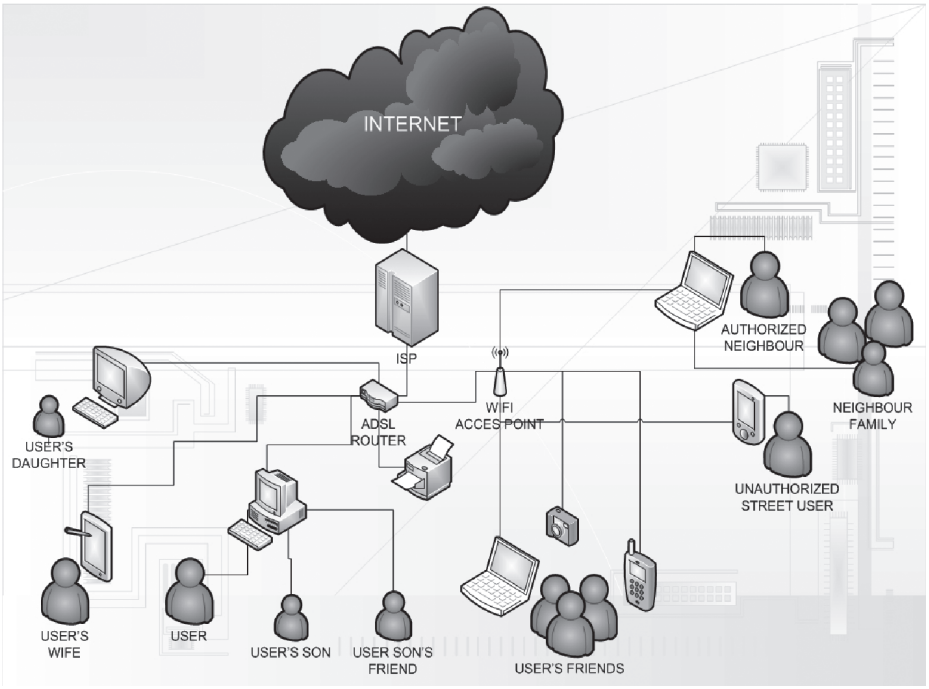
When the user, mainly the classic user, considers that everything can be done, then the reaction of regulators is to limit some possibilities. But here comes a new misconception, from the legislators' point of view (Figure 2). Regulators consider that the ISP is responsible because it knows exactly who the user is and what the user does. And this is not true. The ISP only knows who pays the service, but it can't say if there is only one person using that user account. There might be many different persons with the same line (Figure 3):

Let's imagine a house, Alice lives there and she is a mother who pays the Internet account. Alice has a computer and she does not worry about security. They have only one account and all the family uses it. The son does his homework and sometimes some friends come to work together. Furthermore, the father of that family uses his PDA to connect to Internet. Their daughter also has another computer in her room, and sporadically some friends come to the house with their own laptop. One of them is a geek and has a SD (Eye-Fi[2]) that connects automatically with the WIFI access point and sends the photos to Internet. Alice is a good neighbour. She shares her connection with a neighbour that has promised her to use it for email, but the neighbour's children have not

2. SD with WIFI connection: http://www.eye.fi/overview/index.html

promise anything. And finally, there's a bar with a terrace in front of Juan's home and where some people try to and get access to his connection.

Figure 2. An example of a possible Internet account use



In short, at least 7 different persons can connect to Internet with Alice's account. And we have not taken in account the printer that automatically connects with the technical service if it detects any problem. We can also add a fridge with Internet connection. This is not science fiction: someone has even excused crimes alleging that it was due to his pet[3]. It is easy to see that end-wire users (final users who use Alice's router to reach the Internet through Alice's ISP) are transparent to the ISP itself. Due to technical limitations or features of the IP protocol (IPv4 has an insufficient number of IP addresses to reference all current Internet users; Network Address Translation (NAT) solves it assigning one –and only one– IP address to all users using Alice's subnet), the number of users or their identity far away from Alice's router is totally unknown for the ISP. So, the ISP could avoid some responsibilities and make Alice responsible of any user (known or unknown to her) using her account.

3. Some people do not bother to accuse their own pet: http://www.nbcmiami.com/news/local-beat/Man-Naughty-Kitty-Downloaded-Kiddie-Porn-52640667.html

Imagine that in Spain we want to make Telefonica, and the others ADSL providers in charge of all the people connecting with their services. More than five million lines have ADSL contracted[4]. If we include business, then there are more than nine million lines.

2. Industry wants to ban a woman from downloading ("access" and "download" are technically synonyms)

After a federal judge ruled that a woman accused of sharing over 1700 song had to pay $1.92 million, the Music Industry wants now to ban that woman from downloading[5]. This is not easy to implement. For example, you can ban her user, her name or ID and make impossible to her to contract any service, but she can steal the Internet of a neighbour, or she can contract Internet with a name of a relative. Then we can use something like MAC (Media Access Control) address, and block that address from the Internet, but she can change the MAC address, or buy another network adapter. So, then, we will have to prohibit her to buy any adapter or device that can be connected to Internet, but then someone can give her a Smartphone or any similar device as a present and she will have access to Internet again. So we will have to contract an inspector to watch her house and monitor that no one lets her to connect to Internet and download anything. But she can go to an Internet coffee and download something to a pen drive, so we will have to have a fulltime employee keeping an eye on her. The easiest would be to keep her in a dungeon. Why not? She would not be left there to stop her from seeing the light of the sun, but because the castle's walls impede good coverage. However, that solution would imply cutting her freedom for more than "don't let her download again".

In IT, and more precisely in computer network language, the words "access", "upload" and "download" are technically synonyms. Accessing a website, for example, consists of uploading a request to a web server and receive a download (possible a HTML document), which is the web document that we finally see in a web browser. With this in mind, it is easy to see that banning someone from downloading Internet content is banning him or her from accessing any Internet content. To sum up, this means banning him or her from using almost any electronic device, which is not feasible nowadays.

3. FACUA accuses Microsoft, Yahoo and Google for low security in the access to email accounts

FACUA has informed the Spanish data protection Commissioner (AEPD) that Microsoft, Yahoo and Google do not respect the Spanish Data Protection Act[6].

4. More exactly 5.598.691: http://www.cmt.es/es/publicaciones/anexos/I_Trimestral_09_OK_.pdf
5. http://arstechnica.com/tech-policy/news/2009/06/jammie-thomas-retrial-verdict.ars.
6. https://www.facua.org/es/noticia.php?Id=3774.

FACUA does not blame those companies for having a bad encryption mechanism, or a bug that makes easy the access to other people's account. What they say is that the mechanism of the "security question", used to in case of having forgotten the password, is not trustful. That mechanism is provided to help the user and relies on the user. The "security question" asks the user to select a question from some predefined (as "What's your favourite pet's name?", "What's your primary teacher's name?" and similar) and provide the answer to them. But if the service provider asks the user to choose one question the user is not forced to answer sincerely that question. This gives the service provider a way to help the user if he forgets the password. The user may write what he wants in the answer: a more complicated password, a fake answer, the real one but writing numbers between the letters and many other options. The solution that FACUA propose is to give another email address to have the password sent in case the user asks for it. This requires that the user has a second email address and a different password from the one that is forgotten. Indeed, if the two email accounts have the same password and both email addresses are used as a backup address, you have lost the two accounts. Common sense is also useful in Internet. If you are a famous actress and you have a dog and everybody knows how much you love your dog, please do not use as security-question "What's your favourite pet's name?", as Paris Hilton did[7].

4. Germany will block by law online children pornography

Germany is going to install some kind of software that will block the access to child pornography web sites[8]. This would be very beautiful if it was possible, but this would be like blocking all the content of one kind. All the authoritarian countries would pay a lot for this software, because they would be able to block what they do not want to be accessed by their people. For the moment, it is not possible. Furthermore, paedophiles usually share their data using private channels like forums, or they send via classical mail DVDs. There is no intelligent software that can discover if the images of a website or the videos are classified as child pornography. We can imagine that paedophiles will neither buy the domain www.childporn.com or www.paedophilesclickhere.com, nor will name the files childporn.jpg childporn2.jpg. So what can be done is to block known websites, as the Spanish Science and Technology Ministry did with the Euskal Herritarrok sites. For the moment, we cannot automatically detect new sites. Someone has to monitor the whole web if we want to avoid people to connect to any worldwide site, not only the German ones. If Germany is the only country to block, then we could avoid the effects of the measure with a

7. How Paris Hilton account was hacked: http://www.oreillynet.com/pub/a/mac/2005/01/01/paris.html
8. http://noticias.terra.es/Economia/2009/0325/Actualidad/Alemania-bloqueara-por-ley-la-pornografia-infantil-online.aspx

web proxy server. A proxy is a machine that provides you with the content you are trying to get. Nevertheless, your ISP detects that you are only connecting to the proxy. The same can be done with the prohibition to visit the Euskal Herritarrok sites in Spain. The only condition is that the proxy server has to be outside Spain.

5. Social Networks, YouTube and similar

Judges, prosecutors and politicians have realized that social networks can be used to help extremists or to practice bulling and many other misuses[9]. Yes, it's true, but why do we only blame the service providers? We can also blame the mobile phone makers because with a mobile phone and a camera, recording a video of a violent aggression to a school mate is much easier than recording it with a steady-cam. And with the extremists using social networks, it is obvious that they will used every method that helps them to communicate. We are not saying that the user of social networks has to be free of control. However, is too easy to say "we are going to control all the traffic of the social networks to avoid future terrorist incidents". The problem is how are we going to monitor more than 250 million users of Facebook[10]? How privacy is going to be respected? Furthermore, would it be useful if they use an invented language or communicate with themselves with codes like "changing the state of Facebook means that I'm ready to operate"?

6. Conclusions

It is not easy to match our desires with reality. The majority of people would be happy with an Internet without child pornography or without terrorists, a world without children bulling their classmates and recording it with the phone and posting it to YouTube. But is it a problem about Internet Service Providers, or is it about child pornography, terrorism or bullying? So the best solution is education, not only education of the children about violence and sex, but education for everybody. Lawmakers who have to rule laws about technology must know a bit of it to avoid the goal of monitoring "all the traffic of internet". We should be concerned, while writing this paper we used the Internet to find information about child pornography, terrorism and so on. We could be classified as dangerous people. As stated before, finding exactly who is at the end of the connection is difficult. So, ISP responsibility is the easiest and the wrong option.

9. http://iblnews.com/story.php?id=46447.

10. http://www.facebook.com/press/info.php?statistics.

Many people in our days prefer having free things than privacy: many applications in Facebook ask to provide access to your data to get the results, and many people do it. So, people firstly have to be aware of this fact and protect their privacy.

In a world that changes so fast, where everyday borders are more diffused, it is going to be difficult for the lawmakers and politicians to do their job. They have to change their minds and try to be near to technology and all the new discoveries: regulation includes technological issues. Unless everybody has a chip installed in their bodies and we can only connect to internet with this chip, it is going to be difficult to know who exactly is doing illegal actions. But if that moment arrives, be sure that there will be a black market to change or to have more chips o to get access to the Internet.